

BENCHMARKS

The Newsletter of the University of
North Texas Computing Center

VOLUME 11 NUMBER 4
June 1990

Security, Social Responsibility and the Appearance of this Newsletter

By Claudia Lynch, *Benchmarks* Editor (BITNET: AS04@UNTVM1)

The focus of this issue of *Benchmarks* is security and social responsibility. Computers have become increasingly important in our everyday lives, both in and out of the workplace. It is essential that people be cognizant of the importance of securing their computer systems, both hardware and software. Many of the articles in this issue speak to those needs.

Of perhaps even greater importance is the necessity to be a responsible computer user. This means resisting the temptation to write "cute" programs that will disrupt others' computer systems, not sending "junk" and/or potentially threatening messages over computer networks, not using computer networks for criminal activities, etc. Three articles this month give graphic illustrations of irresponsible computing. They are "Detective Story Traces Hacker to Scene of Crime," "WAN Security & Viruses," and "The Secret Service, UUCP, and The Legion of Doom." The 1990's have been heralded as the decade of connectivity. If this is to be true, then a heightened sense of social responsibility must prevail. If this does not occur, the connections that have been established will be severed, and computer systems will return, for the most part, to the isolated entities that they were in the past.

On a brighter note (I hope), *Benchmarks* is undergoing a transformation. Due to the costs and poor print quality associated with having a pre-printed color page, we have decided to fall back to the more traditional black and white model you have before you now. While I was changing the cover page, I decided to change a few other things also. I will probably change a few more things before the summer is over, resulting in what I hope will be a more appealing and legible newsletter. If you have any comments or suggestions regarding our new look I would be glad to hear them. My various addresses are printed throughout the newsletter. Drop me a line. Your suggestion could make the difference in the appearance of *Benchmarks* for a long time to come. §

Focus of this Issue:
**Computer Security and
Social Responsibility**

TABLE OF CONTENTS

GENERAL INFORMATION

Academic Mainframe Operating System Upgrade Report	3
Saving Files on Academic Disks	4
Staff Activities	5
How Secure Is Your User-Id?	5
Detective Story Traces Hacker to Crime	7
WAN Security & Viruses	7
The Secret Service, UUCP, and the Legion of Doom	10
More Internet Databases	16
The BITNET Connection	15
LIST of the Month	17
Benchmarks Forum	18
Faculty, Staff Seminars	19
1990 Summer Short Courses	19

MICROCOMPUTERS

Maczilla -vs- the Slime Monsters	22
Macintosh ZUC Virus	22
WordPerfect Users Group Meetings	23
MICRO-TIPS	23
Safe Computing Thwarts Viruses	27
Nasty Mac Trojan Discovered in Canada	28
Protecting Your Computer Hardware & Peripherals	29

VAX COMPUTER CLUSTER

VAX Upgrades	30
Best of the BBS	32
VAXcluster Usage Statistics	32

COMPUTING TECHNICAL SERVICES

Mainframe Security	33
Performance Statistics	34
Program Hit Parade	35
Disk Backup Schedules	36



SERVICES AVAILABLE TO USERS OF THE UNT COMPUTING FACILITIES

The UNT Computing Center is located in the Information Sciences Building (ISB), Room 119. Phone Numbers:

Computing Center: (817) 565-2324
Help Desk: (817) 565-4050
Micro Support: (817) 565-2316, 565-2319
Graphics Lab: (817) 565-3479
ISB I/O Area: (817) 565-3890
BA I/O Area: (817) 565-2350

All personnel listed below can be contacted either by calling the Computing Center or by sending them electronic mail on MUSIC/SP (ID-codes follow each name. All IDs are on BITNET node UNTMUSIC).

Benchmarks - Claudia Lynch (A804)

Information & ID-Codes; Disk Space Problems - Theresa Russell

Statistical/Research Support - George Morrow (A801), Panu Sittiwong (AC09), Phanit Laosirirat (AC44)

Academic ADABAS/COM-LETE - Cathy Hardy (AC55)

CRSP & COMPUSTAT Problems - Panu Sittiwong (AC09), Phanit Laosirirat (AC44)

Student Programming Problems - CSCI Dept., GAB Room 550; BCIS Dept., BARoom 152

Problems with JCL, Passwords, or Operating Systems; or Communication/Terminal Problems - Help Desk

Data Entry; Test Scoring & Analysis - Betty Grise

Administrative Applications - Coy Hoggard

Printout Retrieval - ISB or BA I/O Operators



DIALING-UP UNT COMPUTERS OVER THE TELEPHONE

Phone numbers for the Local Area Network (LAN) are:

300 - 2400 BAUD: (817) 565-3300
 300/1200 BAUD: (817) 565-3499
 300 - 9600 BAUD: (817) 565-3461
 300 - 9600 BAUD: D/FW METRO 429-6006, 429-9314

Area code 214 must dial 817 before the METRO #.

The numbers that accommodate multiple baud rates have an autobaud feature that requires you to hit the <RETURN> key repeatedly so that the receiving modem can determine the appropriate baud rate. When you have established a communications link, the # prompt will appear on your screen and you can enter one of following CALL commands to connect with the computer of your choice.

CALL 8040 connects with the HDS/8083 (supports line editing or PCWS). Operating environments available are: MUSIC/SP, VM/CMS.

CALL 3270 connects with the HDS/8083 through a 3270 protocol converter (supports full-screen editing). Operating environments are: MUSIC/SP, VM/CMS, ADABAS/COM-LETE

CALL DEC connects with the VAXcluster (VMS, Eunice)

CALL 780 connects with the Research VAX (Unix)

CALL 3000 connects with the Libraries' HP-3000 (Bibliographic database).

CALL 6800 connects with the NBI (Unix)

Communications Settings

LAN addresses	Data Bits	Parity	Stop Bits
DEC, 3000	8	N	1
8040, 3270, 780, 6800	7	E	1

HOURS FOR UNIVERSITY OF NORTH TEXAS COMPUTER ACCESS AREAS : Summer 1990*

Location	Days	Times
Computing Center RJE	Sunday Monday Tuesday-Saturday	Noon-Midnight 7 a.m.-Midnight 7 a.m., Tues.-Midnight Sat. (Open 24 hours/day)
ISB 110 Terminal Area	Sunday Monday-Thursday Friday Saturday	1 p.m. - 10 p.m. 8:00 a.m. - 10 p.m. 8:00 a.m. - 6 p.m. 9 a.m. - 6 p.m.
College of Business	Sunday Monday-Thursday Friday, Saturday	Noon-11:45 p.m. 8:15 a.m.-11:45 p.m. 8:15 a.m.-7:45 p.m.
GAB 550C	Sunday Monday-Thursday Friday Saturday	4-11 p.m. 9-11 p.m. 9 a.m.-3 p.m. CLOSED
Graphics Lab	Sunday Monday-Thursday Friday Saturday	Noon-10 p.m. 7 a.m.-10 p.m. 9 a.m.-6 p.m. Noon-6 p.m.
Willis Library	Sunday Monday-Thursday Friday Saturday	1 p.m.-10 p.m. 7:30 a.m.-10 p.m. 7:30 a.m.-9 p.m. 9 a.m.-9 p.m.

*Hours may vary. Check MUSIC/VAX News and/or posted schedules for exceptions.

This issue of Benchmarks was produced by the Documentation Services section of Academic Computing, using Xerox Ventura Publisher on an AT clone and printed on an Apple LaserWriter II and an HP LaserJet Series II. Unless otherwise noted, articles or information may be reproduced for nonprofit purposes provided the publication and issue are fully acknowledged.

Academic Mainframe Operating System Upgrade Report

By Dr. Philip Baczewski, Academic Mainframe User Services Manager
(BITNET:AC12@UNTVM1)

Question: *How many systems programmers does it take to change a light bulb?*
Answer: *None; that's a hardware problem.* That might be a pretty good joke, but it doesn't quite reflect the realities of maintaining a large computing system. Hardware and software are inter-dependant, and both areas must be taken into account when any major operating system change is made to the mainframe. This is especially the case in upgrading from VM/SP to VM/XA. During the three-week semester break following the spring semester, the UNT Computing Center was involved in installing VM/XA on the academic mainframe computer, a project which was discussed in the April/May issue of *Benchmarks*.¹

As stated in that article, this time period was chosen to try to avoid a disruption of mainframe computing services during the summer terms. It was felt that the semester break offered the best chance of inconveniencing the fewest number of users during a process which would require three or more days of system down time and periods of system instability immediately after the installation was accomplished. As was stated in the previous article, immediately after the upgrade the mainframe would still be in a "use at your own risk" status. The installation process turned out to be every bit as difficult as anticipated, and more.

Why so Much Down Time?

In order to run VM/XA on the HDS 8083, the dual cpu system had to be reconfigured to support the newer software technology; new micro-code (the "lowest-level" software on the system) had to be loaded to support the new operating system. Because VM/XA utilizes a different mainframe architecture than VM/SP, the new VM system had to be "built" from a very basic level, and that process could only be started after the necessary changes were made to the hardware.

The question can be asked, "why couldn't the basic VM/XA system be built before the upgrade process began?" When UNT upgraded from VM/SP version 3 to version 5, the initial installation could be done under the control of VM/SP version 3. This approach is not possible with our present upgrade to VM/XA because the computer architecture required for VM/XA is different from that required for VM/SP.² It is not possible, therefore, for VM/XA to "run under" VM/SP (however, it is possible for VM/SP to run under VM/XA, since VM/XA can simulate the architecture require by VM/SP).

¹ See "VM Upgrade Planned," on page 11 in the April/May, 1990 issue of *Benchmarks*.

² *Computer Architecture* can be defined as "its attributes as seen by the programmer; that is, the conceptual structure and functional behavior as distinct from the organization of the data flow, and logical design, and the performance of any particular implementation. Several dissimilar machine implementations may conform to a single architecture. When programs running on different machine implementations produce the results that are defined by a single architecture, the implementations are considered to be compatible." For more information on IBM mainframe architecture, see *IBM Mainframes, Architecture and Design* by N.S. Prasad.

Another approach might be to build the initial VM/XA system on a physically-separate computer system similar in configuration to the HDS 8083. In reality, however, the UNT Computing Center does not currently have the budgetary resources to acquire an additional mainframe computer for this purpose. Therefore, the only course of action available in this case for performing the upgrade to VM/XA (and likewise, the only way to utilize the full performance capabilities of the HDS 8083) was to shut the machine off from the academic users to perform the upgrade on the academic mainframe. Under the best of circumstances, reconfiguring the mainframe and building and installing the new operating system would take at least two to three days. As academic mainframe users are painfully aware, UNT's initial upgrade process required almost seven days of system down time.

What Happened during the Upgrade Process?

The upgrade began on Wednesday, May 16, with Hitachi Data Systems staff reconfiguring the HDS 8083 to support the VM/XA architecture. By Wednesday afternoon, the first steps were being taken to load a "starter system" onto mainframe disk drives. Problems were encountered with this process, however, and it was finally determined that the program supplied to us by IBM for this purpose was the wrong version (IBM's mistake). IBM agreed to send the correct version by the next day.

On Thursday, May 17, the starter system was loaded on to disk. Attempts to IPL³ the VM/XA system in multiprocessor mode (i.e. to use both CPUs on the HDS 8083) were unsuccessful. It was determined that HDS staff would need to make further changes to the micro-code. The new micro-code was loaded on Friday, May 18, and by Friday afternoon, we were ready to proceed with installing the VM/XA system. By this time, almost three complete days had been occupied with resolving hardware and software incompatibilities.

VM/XA was up and running by Sunday, May 20, however, it took a bit more time to bring up the production VM/SP system under the control of VM/XA. It took Monday and part of Tuesday to resolve problems encountered when trying to bring up MUSIC and MVS. MUSIC came up at about 1:30 p.m. on Tuesday (May 22) and MVS was started at about 5:30 p.m.

Why Wasn't There an Immediate Improvement in Mainframe Performance?

The HDS 8083 can now run VM/XA version 2.1 as its primary operating system utilizing all 32M of the machine's memory as well as both processors. Please note, however, that VM/XA upgrade process is not scheduled to be completed until August (see the previous article in the April/May issue). Because this intermediate step requires VM/SP to be running under the control of VM/XA, there will be no noticeable performance gains before the final phase of the upgrade, when VM/SP can be removed and full utilization can be made of VM/XA.

Because the first stage of the upgrade was incomplete, immediately after VM/XA was installed we actually

³ IPL stands for Initial Program Load. An IPL is the process used to start a mainframe operating system running.

Saving Files on Academic OS Disks

By George Morrow, Academic Computing Consultant

This is a reminder of the policies concerning the storage of files on the academic OS disks: ACAD00, ACAD01, ACAD02, and ACAD03. The designated use of these disks is as follows:

ACAD00	faculty research
ACAD01	College of Business instruction
ACAD02	all other instruction
ACAD03	faculty research

When storing a file on one of these disks you must use the following University of North Texas naming convention. The convention is of the form: USER.IDxx.name

where:	USER	must appear
	.	must appear
	IDxx	is your user ID
	.	must appear
	name	one or more optional fields (each of which may not exceed 8 characters), separated by periods.

The total length of the data set name may not exceed 44 characters, including the first three mandatory fields and any periods. Usually the larger the blocksize, the more efficient use of disk space. Please do not write data to disks with a blocksize of 80 or less, 4800 is an efficient blocksize to use with logical record of length 80.

At the end of each semester any files on the academic disks that have not been referenced (read) in the past six months are archived to tape.§

experienced a level of VM/SP system performance lower than before the upgrade began. The academic mainframe system was shut down at 8:00 a.m. on Saturday, June 2, and was not restarted until 8:00 a.m. on Monday morning, June 4. This downtime was necessary to try to improve system performance of VM/SP and was a necessary part of the VM/XA upgrade process. Once the entire process is completed in August, the full benefits of the VM/XA upgrade can be realized.

Why Change?

Perhaps you've heard this one:

Question: How many psychologists does it take to change a light bulb?

Answer: One, but the light bulb has to want to change. Change has become inevitable in our increasingly complex technological society. Installation of VM/XA on the academic

mainframe is being done to better support the changing needs of instructors and researchers using that system. These changes are both in reaction to present problems and in anticipation of future needs.

Much work has gone into the installation of VM/XA, yet much work remains to make it the "production" environment of the academic mainframe. With VM/XA comes a new CMS system as part of it, on which many programs are yet to be installed. This work will proceed through the summer and by the fall, it will be possible to eliminate the VM/SP "middleman." The Computing Center realizes that any time the academic mainframe is down it is probably an inconvenience to someone. We are working to keep the inconvenience to a minimum and we appreciate the patience of our academic mainframe users.§

Computing Center Staff Activities

The Computing Center staff has been busy doing many things in addition to their normal job duties. Following is a list of staff members and their various accomplishments.

- Dave Molta, Director of Academic Computing, gave a paper at the 1990 Network Users Conference in Dallas on May 15. The title of his presentation was "Common LAN Problems." Dave also has had the pleasure of seeing his book, *Novell Netware: Advanced Techniques and Applications*, published. Co-authored with Dr. Paul Schlieve of Computer Education and Cognitive Systems, the book is available in paperback from Wordware Publishing, Inc.
- Chandrabhan (C.R.) Chevli, Data Communications Analyst, presented a paper at the International Conference on Computing and Information (ICCI'90) at Niagara Falls, Ontario, Canada (May 23-26). The paper, co-authored with Hee Yong Youn of the Computer Science Department is entitled "An Efficient VLSI Network Bridge Architecture for Local Area Networks." The article was published in *Advances in Computing and Information*, the Proceedings of ICCI'90, and will be included in a forthcoming book called *Lecture Notes*, from Springer Publishing Company.
- Scott Norton, Linda Wallace, Sue Harrison, Margaret Ambuehl, Dierdre Hayes, Jenny Haynes, Mashid Grooms, Rocky Bass, Eric Duchemin and John Dysart continue in their pursuit of physical fitness. Norton, Wallace, Harrison, Ambuehl, Hayes and Haynes all received t-shirts for their attendance of 40 fitness classes during the Spring 1990 semester. Linda Wallace logged 272.0 miles while walking/jogging indoors. She also won first place in her age group in the Broncos Against Drugs 5K on February 17. Other indoor walker/joggers (Pace-Makers) and their distances include: Scott Norton — 219.0 miles; Margaret Ambuehl — 123.0 miles; Deidree Hayes — 97.0 miles; Jenny Haynes — 87.0 miles; Mashid Grooms — 84.0 miles; Rocky Bass — 83.5 miles; Sue Harrison — 71.0 miles; Eric Duchemin — 18.5 miles; and John Dysart — 11.0 miles.
- Philip Baczewski may have the distinction as the first *Benchmarks* author to have an article translated into a foreign language. His "BITNET Connection" article "Is Anyone Out There?" (*Benchmarks*, October 1989) was translated by Pablo Liendo for use in Caracas, Venezuela. The Spanish title is "¿Hay Alguien Allí?" If, by chance, you would like to see this in Spanish, we have a copy.

On the job front, the following activities have occurred:

- James Shoffit, longtime VAX Lead Operator, BBS author, and general wizard, made us realize just how good he was when he left to take "a real job" (he was part-time) at Atlas Powder Co. in Dallas.
- Abraham John decided that he preferred microcomputers to mainframes and returned to his job in the Dean of Students office. Cathy Hardy has joined the Academic Computing staff as Abraham's replacement. Cathy was employed with the Database Central Programming Support Team (CPST) in Administrative Computing and *knows* she likes mainframe computing.

How Secure is Your User-id?

By Dr. Philip Baczewski, Academic Mainframe User Services Manager
(BITNET: AC12@UNTVM1)

The people that write computer operating systems have long realized that data security is a desirable and necessary part of any multi-user computing system. That's why most systems won't allow you access unless you give some type of password known to both you and the computer operating system. Operating systems employ varied schemes for keeping these passwords a secret, in some cases, only storing an encrypted version of the password on line. A great deal of responsibility for user-id security is also placed upon the shoulders of you, the computer user.

Selecting your Password

How you select your password and how you protect it will, to a large degree, determine how secure your user-id is. The ideal password is one which is meaningful enough to you that you can recall it from memory, yet not something so related to you that someone could guess it. Possibly the worst password you could pick is your first or last name. (Actually, the very worst password would be the user-id itself!) Anyone who happened upon a listing of your name and user-id would not have a difficult task if their intent were to "break into" your user-id. Likewise, the names of spouses, children, or pets are not necessarily the best choices either. Perhaps a random set of letters and numbers is the best password, however, this is definitely not the case if you have to have your

Do not give out your user-id and password over the phone or via an on-line interactive or mail message.

password written down next to your terminal in order to remember it.

How, then, do you select a secure password? A password should probably consist of a combination of more than four letters and numbers, and, if the system allows it, special characters such as punctuation marks (inclusion of numbers or special characters decreases the likelihood that your password could be guessed by someone running a "dictionary program").¹ Another password possibility is to think of a phrase which is well-known to you and combine the first letter from each word to form the password. This usually results in a combination of letters which is hard for someone else to guess, yet easy for you to remember.

Keeping your Password Secure

Once you select and use a secure password, your user-id will be totally secure only as long as that password is known only to you and the computing system. If you write down your password in a place where others might see it, you are jeopardizing the integrity of whatever information you have stored on your computer user-id. Sometimes it is necessary for two or more people to gain access to one user-id. In this case, each person knowing the password should be as careful to protect it as if it were their own personal user-id involved.

¹ One method computer hackers use to break into systems is to write a program which will read words from a dictionary and then try them as passwords for known computer userids. [Keep reading this issue for more information on this — ed.]

In keeping your password secure, you should also follow these additional guidelines:

- Do not give out your user-id and password over the phone or via an on-line interactive or mail message.

No matter why callers say they need it, do not reveal your password or anyone else's password. Do not be intimidated into telling them regardless of the reasons they give. Generally, the administrator of any system you use has sufficient privileges to resolve any problem with your user-id.

- Be suspicious if callers or other on-line users identify themselves as Computing Center personnel and demand your password over the phone or on-line.

Be suspicious if callers or other on-line users identify themselves as Computing Center personnel and demand your password over the phone or on-line.

No Computing Center personnel will ever demand your password. Any problem that needs to be resolved by Computing Center personnel can be referred to the appropriate system administrator and should not require that you divulge your password.

- Report any attempts to obtain passwords to the appropriate system administrator.

Reporting such an attempt to the system administrator will allow him or her to be on guard for someone attempting to compromise system security.

Changing Your Password

Any time you think your password may have become known to someone else, you should immediately change it. Sometimes it is best to change it on a regular basis to guard against accidental discovery. When changing your password, be sure to memorize it. Computing Center personnel can change your password to an agreed value if you have forgotten it, however, this is an inconvenience to both you and the Computing Center. Also, just as you should never give out your password over the phone, Computing Center personnel will not give you your password over the phone. In order to protect the security of your on-line information, we will only give you your password if you come to our offices and show some type of photo identification card.

There is some difference of opinion among system administrators as to if passwords should ever expire or not. Some make the argument that expiring passwords on a regular basis encourages people to write them down, thus lessening system security. Some think, however, that if the expiration period is of a reasonable length, automatic expiration can guard against accidental discovery of passwords. On UNT's MUSIC system and on the VAX Cluster, log-on

GENERAL INFORMATION

passwords do not expire. On CMS, passwords expire after 180 days and MVS/SP passwords expire in anywhere from 30 to 180 days (as set by the user).

The Bottom Line on Password Security

In the final analysis, the security of your user-id is ultimately determined by you, the computer user. Software systems and system administrators go to great lengths to prevent unauthorized access to user-ids. If your name is Fred Smith, your user-id is "SMITH," and your password is "FRED," you've just short-circuited all of that protection in one simple move.¶

Detective Story Traces Hacker to Scene of Crime

By Christine de Aragon (CDEARAGO@ORION.CAIR.DU.EDU) *Buffer* Editor
University of Denver.

This article originally appeared in the University of Denver Computing Center Newsletter, Buffer (Volume 25, Number 1 January 1990). It was received from the Articles database of CCNEWS, the Electronic Forum for Campus Computing Newsletter Editors, a BITNET-based service of EDUCOM. The Cuckoo's Egg; Tracking a Spy Through the Maze of Computer Espionage, was written by Clifford Stoll and published by Doubleday Books. It is available in most major bookstores.

The recently published book, *The Cuckoo's Egg*, has all the elements of a classic spy novel but the detective is a hippie astronomer who follows a trail of clues through a computer network.

Continued on page 8.

Changing Your Password on Different Systems

If you need to change your password, the following information may come in handy:

SYSTEM	PASSWORD CHANGE METHOD
VAX/VMS	Use the Set Password command. The Vax will prompt you for the information needed to change the password.
MUSIC/SP	Use the PROFILE NEWPW command. MUSIC will prompt you for the information needed to change the password.
VM/CMS	Use the DIRM PW command. The Directory Maintenance program will prompt you for the information needed to change the password.
MVS/SP	Use the CHANGE PW utility program on MUSIC or use the format <code>PASSWORD=(old_password,new_password)</code> on your MVS JOB card.
Unix systems	On the Unix systems (RVAX or NBI) use the passwd command. The system will prompt you for the information needed to change the password.
Novell file servers	To change your Novell file server password, use the SETPASS command or optionally SETPASS server_name. The file server will prompt you for the information needed to change the password. If you specify only SETPASS, you will be able to change the password on the server to which you are logged onto and optionally be able to synchronize your password on all servers to which you are attached.¶

WAN Security & Viruses

By Billy Barron, VAX System Manager (BITNET:BILLY@UNTVAX)

Due to the exponential growth of Wide Area Networks, viruses and security problems on WANs has become a major issue. To start our investigation of these issues, let's first look at the history of WAN security and viruses.

History

The Christmas Virus

Around Christmas time in 1987, the first major WAN virus appeared and was immediately dubbed the Christmas virus. The Christmas Virus was a REXX (CMS) script that drew a Christmas tree on the user's screen. Meanwhile, it would look in the user's NAMES file and find the addresses of other network users. Once these addresses were found, the virus would send copies of itself to those users. Fortunately, the only purpose of the virus was to propagate itself. Because of all the copies of the Christmas virus, it greatly slowed down BITNET and bought VNET, IBM's internal network, to its knees.

Continued on page 8.

Detective Story continued from page 7.

The Cuckoo's Egg, written by Clifford Stoll, is a true, detailed account of Stoll's involvement with international computer espionage told with wit and humor.

Although the images of a textbook spy, dressed in a trench coat and without a sense of humor, enters our minds and Stoll's alike, the methodical hacker remained faceless and was only identified by his passwords throughout the majority of the book.

This is not the typical cloak and dagger book with secret decoder rings and murder. Instead Stoll writes about networks, military computers, Trojan horses, Unix and VMS.

Computer security is a serious matter. Even though Stoll provides a technical analysis, he often approaches the topic lightheartedly and even humorously.

For example, he describes the password encryption software as "a one-way trapdoor; its mathematical scrambling is precise, repeatable and irreversible." But then he compares it to a sausage machine; "if you turn the crank backwards, pigs won't come out of the other end."

The narrative provides a history lesson in Unix and VMS with other technical information to be appreciated by computer wizards. Yet the story is well written and can be easily followed by computer novices.

Stoll was an astrophysicist turned systems manager at Lawrence Berkeley Lab in California when a 75-cent accounting error alerted him to a hacker with super-user privileges.

The intruder moved through a maze of American military and research computers unseen by most, but tracked by Stoll. A year of stalking lead Stoll to West Germany where he set up a sting operation and uncovered a spy ring.

Stoll viewed the 75-cent shortfall as a natural test for a budding software wizard. He discovered the hacker had exploited bugs in the Unix and VMS systems to cruise through the networks free of charge and unnoticed.

On the Unix computer, the hacker found a bug in the Gnu-Emacs editor. He used Gnu to swap his special atrun file for the system's legitimate version. Within five minutes the bogus file would be operational, giving the hacker the keys to all the doors in the system.

The hacker was like a cuckoo bird; laying eggs in other birds' nests. The survival of the cuckoo chicks depends on the ignorance of the other species to raise the young. The hacker laid egg-programs, let the system hatch it and feed him privileges.

On VMS systems the hacker relied on the carelessness of system managers who failed to change the original passwords. For example, the account SYSTEM, with the password MANAGER, gives the hacker complete privileges.

The hacker didn't pick locks. Instead he preyed on careless system managers who failed to completely secure their computers by locking the backdoors.

By exploiting these bugs the hacker made attacks on about 400 Milnet computers. From Germany, he crossed the Atlantic ocean either by TAT-6 cables on the ocean floor or via satellite through Tymnet, then Lawrence Berkeley Laboratory, across the Milnet to defense contractors and universities across the United States.

This story provides an interesting account of one man's struggle to protect America's military secrets without the help of the FBI, the CIA or any other national agency.

WAN Security continued from page 7.

Eventually, it took three steps to stop the virus. First, the key weakness of the virus was that if users didn't manually run it then it could not spread so users were told to not run this program. Second, many system managers deleted all the copies of the Christmas Virus they could find on their system. Finally, BIT-NIC wrote a virus to find the Christmas Virus and destroy it. This new virus was smart enough to kill itself off after a period of time.

Occasionally, new infections of the Christmas Virus periodically crop up, but they have never been as bad as the original. Modified versions of the Christmas Virus also exist, such as DIR EXEC.

KGB Hackers

In August 1986, ex-astronomer Clifford Stoll at Lawrence Berkeley Labs started tracking down a 75 cent accounting error on their computer system [see companion story on this page — ed.]. Fairly quickly, he discovered that an account had been created on his system without any of the systems people knowing about it. Then a couple of days later, he received a mail message from another site saying that someone from LBL was attempting to break into their computer. Upon further investigation, Cliff discovered that someone had system privileges illegally.

Instead of just locking the hacker out, he decided the best course of action was to allow the hacker to continue using LBL's computer while he would try to track the hacker back to his source. Initial contact with the Police and the FBI led to no results. These agencies only saw the problem as a 75 cent theft instead of the invasion of privacy it was.

Over the next several months, Stoll learned that the hacker was after in-

The most common security hole on Wide Area Networks tend to be return addresses on MAIL.

formation on several military projects and had broken into hundreds of computers on TYMNET and the Internet. Even though Classified information is not kept on networked computers, much can be learned from what is on them. After several gyrations, the hacker was tracked back across the country. Eventually, an FBI agent on the East Coast became very interested in the case. This was a key break.

The trace continued and the hacker was eventually found to be in West Germany. One by one the CIA, the NSA, and the West German Police became involved. Cliff's girlfriend came up with a plan to keep the hacker on the line for a longer period of time. They started creating files about a fictitious secret network called SDINET. Finally, the hackers were caught with this plan.

The hackers turned out to be members of the Chaos Computer Club. The CCC is a group of computer hackers in West Germany that believe that all information should be publicly available. These particular members became involved with selling US military information to the KGB. The West German Police seized the hackers' computer equipment, disks, and printouts. All the hackers but one quit their activities immediately. A year later, some of the hackers admitted their involvement in the incident and helped the police. Charges were brought up against the other members. In the end, three hackers were put on probation. Another one of the hackers committed suicide.

The method used by these hackers involved taking advantage of Unix security flaws and poor password management used by some system

managers. These Unix security flaws have been corrected. Also, during roughly the same time period other Chaos Computer Club members attacked SPAN using bugs in VMS 4.4 security, which have since been fixed.

Internet Worm

Sometime around 6 PM EST on November 2, 1988 the most famous computer virus (technically a worm) in history was introduced into the Internet by Robert Morris, the son of a famous computer security analyst working for the NSA [*Interestingly, Morris Sr. plays an important role in the events described in The Cuckoo's Egg — ed.*]. The worm spread like wildfire infecting hundreds if not thousands of computers in a matter of hours. The only computers that were susceptible were Sun 3 systems and VAXes running BSD 4.3 Unix. Within 24 hours, solutions to stop the worm's

the worm were on some computers that it slowed them down to a halt. The worm took advantage of several Unix security bugs. In addition, the worm attacked password security too. Bug fixes have been distributed for all the security holes. Robert Morris was given three years probation, a \$10,000 fine, and must perform 400 hours of community service work.

The WANK Worm

In mid-October 1989, the WANK (Worms Against Nuclear Killers) worm attacked SPAN (NASA's DECnet network). The goal of the worm was to put a message protesting nuclear war in VMS computers' login screens. The worm utilized all different kinds of attacks. However, it was very easy to destroy and prevent.

Forging Addresses

The most common security hole on Wide Area Networks tend to be return addresses on MAIL. It is possible on BITNET, the Internet, DECnet, UUCP, and possibly on

If you are in doubt whether or not a message has been forged, the easiest way to tell is based on the sender's writing style.

spread had been found. Many sites cut themselves off the network to protect themselves against the worm. Full Internet connectivity was not restored for weeks after this.

The worm's only purpose was to spread itself to as many machines as possible. The original intent was to have only one worm per computer, but due to a bug so many copies of

other networks to forge MAIL addresses. Fortunately, methods for exploiting these problems are not known by most users, but still the potential for havoc is great. Interactive addresses can be forged as well. If you are in doubt whether or not a message has been forged, the easiest way to tell is based on the sender's writing style.

Implementation of WAN Security

Many users expect the Wide Area Network to protect the computers on it from hackers and worms. It is impossible for the network to do this because telling the difference between a legitimate application and a virus is hard for a human much less a computer. A good comparison would be to expect the phone company to make it impossible to place obscene phone calls. Most, if not all, security must be host based.

An important part of this security is good password security. If users pick poor passwords, then a system will be easier to penetrate. A good password should be at least six characters long and not in the dictionary. Bad password choices include your userid and parts of your name. Some systems such as the VAX support a password generator (it can be used by typing SET PASSWORD/ GENERATE), that picks good passwords. Also, never tell anyone else what your password is. Finally, never write your password down on a sheet of paper or store it in a text file on a computer.

Another key is for the System Manager to install security fixes immediately. Related to this is to never run any executable programs from an unknown source. If other users on the network give you a program, it is wise to get the source code for the program, look over the source, and then compile it yourself.

Finally, it is important to keep the number of people that can write files into an account or the system of a computer to an absolute minimum. Unfortunately, many systems take this to an extreme where the computer's useability suffers.

Conclusion

WAN Security is currently a major issue and will continue to be for the next several years. Computer vendors and users alike need to participate in developing and implementing better computer security systems. Unless computer security improves, the Wide Area Networks may have limited growth or even possibly die out over time. §

Lesk and A.S. Cohen and the program they wrote to implement the idea was Unix to Unix Copy, or UUCP. The idea caught on just about the same time Unix was taking off in popularity.

As the number of computers that could UUCP to each other grew, the first wide-area network was born. It slowly grew to the size it has today of over 11,000 nodes, or individual computers. The UUCP network, named after the primary software used for communication across the network in its early days, now provides much more than simple file copying. The UUCP network now provides electronic mail, network-based news services and, of course, file transfer services between each computer on the network.

Electronic mail (e-mail) is a kind of computer-based postal system where people can send messages back and forth to each other electronically without ever having to print them out on paper.

UUCP news is not unlike e-mail. The network of computers where people read, write and distribute news is called Usenet. Most, although not all, of this service takes place on UUCP. Because of its popularity, though, the service is also available from the NSF-Internet and BITNET wide area networks. Usenet news is comprised of several hundred *newsgroups*. These newsgroups are forums for ongoing discussions on an endless variety of topics ranging from specific computer languages and architectures to cooking, horseback riding, politics and religion. When a person sends e-mail to a news group, the message is automatically sent out to every computer on the network that subscribes to that particular news group. That way, each person who reads and posts to a news group is literally carrying on a dialogue with hundreds, often thousands, of other people at the same time.

The Secret Service, UUCP, and The Legion of Doom

By Kevin Mullet, Data Communication Analyst (BITNET: KEV@UNTVAX)

UUCP

Back in 1978, a couple of bright fellows at AT&T's Bell Labs, where the Unix operating system was developed, wondered if computer files could just be copied from one computer to another over a cable. State of the art data transfer back then meant writing data to paper cards or magnetic tape and reading them in on another computer. The chaps with the bright idea were M.E.

prevent you from reading any of your messages. If you wish further information, type **HELP MAIL** at **MUSIC *GO** mode, or read the help information provided as part of the **MAIL** facility (**PF1**).

Sending and Receiving BITNET Mail on CMS

The CMS mail system allows you to send and receive mail, manage log files containing mail messages, and set up a names file containing nicknames for BITNET addresses. The three programs that perform these functions are respectively **MAIL**, **MAILBOOK**, and **NAMES**. A complete description of these programs may be obtained by typing **HELP name** at the CMS command prompt, where **name** is the name of the program for which you want information. You can also refer to the document *A User's Guide to Electronic Mail on CMS*, available at the Computing Center offices (ISB 119).

The format for sending BITNET mail on CMS is **MAIL userid AT node** or **MAIL userid@node**. Note, however, that CMS normally interprets the **@** character as meaning "delete the previous character." If you wish to use the second form of BITNET address, you must disable or change the CMS "delete character" by entering one of the following commands when you first log on:

TERMINAL CHARDEL OFF
(to disable the delete character)

TERMINAL CHARDEL %
(to change the delete character- in this example the delete character has been changed from **@** to **%**)

Either of these commands may be included in your **PROFILE EXEC** file. CMS **MAIL** will prompt you for optional "To:" name, "From:" name, and "Subject:" fields and then allow you to enter your message text.

Typing **MAIL** without any address specification will instruct the **MAIL** program to check your CMS reader for any incoming mail messages. If you have received any messages, **MAIL** will enter its "read" mode and display a list of incoming mail.

To create or modify a "names" file containing your list of nicknames, you type **NAMES** from the CMS command prompt. (For help within the **NAMES** program, use **PF1**.) If, for example, you frequently send mail to **HARRYX** at **CZHRZU1A**, you could define the nickname **HARRY** to represent that address. To send mail to that address, you would only need to type **MAIL HARRY**.

CMS **MAIL** can allow the use of "gateway" addresses, that is, mail to

other networks which must pass through a gateway; however, you must do a little work before you can send your mail. Suppose you have a gateway address which has a user-ID and node name which are longer than eight characters, for example, a user-named **Scott** with an address of **USER31EM@UB.CC.UMICH.EDU**. First, type **NAMES** to execute the names program. Type a nickname (**Scott**) for the gateway address in the nickname field of the **NAMES** screen. Next, press **<Tab>** until the cursor has moved to the first "Tag" field and type: **userid** press **<Tab>** again to move the cursor to the "Value" field and type **USER31EM**

Then press **<Tab>** again and type: **NODE <Tab> UB.CC.UMICH.EDU. ARPA**

LIST of the Month

Each month we will highlight one of the BITNET LISTSERV Special Interest Group (SIG) mailing lists. This month's list...

VIRUS-L@LEHIIBM1

Coordinator: **LUKEN@LEHIIBM1** (Kenneth R. van Wyk)
VIRUS-L is a forum specifically for the discussion of computer virus current events, protection software, and other virus related topics. The list is open to the public and is a digest format list.

*This mailing list will keep you informed of all the new Viruses which may show up on various computer systems. Discussions also include how to prevent viruses from spreading and how to disarm various viruses once they have infected your computer system. To subscribe to this list send the following command via interactive message or as the first line of a mail message to **LISTSERV@LEHIIBM1**:*

SUB VIRUS-L <firstname lastname>

GENERAL INFORMATION

The second "Tag" and "Value" fields should now contain the node information. Press PF2 to add this entry to your names file and exit the NAMES program by pressing PF3. You could send mail to that gateway address by typing MAIL SCOTT.

Sending and Receiving BITNET Mail from the VAXcluster

The VAX MAIL utility allows you to send and receive BITNET mail from the VAX Cluster. To send BITNET mail, type MAIL from the VAX system prompt. The VAX will respond with the following prompt:

MAIL>

At this point, you may type SEND and the VAX will prompt you for the information needed to send a message. When you see the "To:" prompt, you will need to enter the BITNET address in the following format: IN%userid@node.BITNET where userid is your correspondent's ID-code and node is their BITNET node name. Once the address has been entered successfully, MAIL will prompt you for an optional subject field ("Subj:") and then allow you to enter your message text. If you had received a BITNET message, you could type READ at the "MAIL" prompt, and MAIL would display the message.

Sending mail through gateways is a bit easier on the VAX. For example, to send mail to someone at an "Arpanet" address, you only need to enter: IN%arpanet_address.ARPA where arpanet_address is the complete designation for the Arpanet user-ID and node. For information on sending to other networks enter HELP NETWORKS at the \$ prompt.

Unlike MUSIC and CMS, VAX MAIL has no names facility, however, you can include logical definitions for your most frequently used BITNET addresses in your LOGIN.COM file. If, for example, you frequently send mail to BARRYZ@JPNKEKVM, you can put the following line in your LOGIN.COM file: DEFINE BARRY IN%""BARRYZ@JPNKEKVM.BITNET""

Then, when you wish to send a mail message to that address, you may type MAIL at the VAX system prompt, type SEND at the "MAIL" prompt, and type BARRY at the "To:" prompt. For more information about the LOGIN.COM file, type HELP GETTING_STARTED from the VAX system prompt.

For further information on VAX MAIL, consult the help information available from within the MAIL program (type HELP at the "MAIL" prompt).§

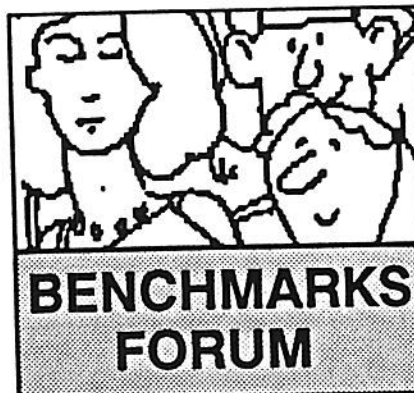
Internet continued from page 16

contains WOCE project information, directories of oceanographic datasets, directories of oceanographers, and oceanographic research ships' schedules. To access OCEANIC, TELNET to DELOCN.UDEL.EDU and login as INFO.

- PENpages - The Pennsylvania Department of Agriculture maintains a database of agricultural in-

formation that is available to Internet users. To use PENpages, TELNET to PSUPEN.PSU.EDU and then login as PNOTPA.

- SDDAS - SDDAS (Southwest Research Data Display & Analysis System) is a large database containing data from the Dynamics Explorer satellites 1 & 2. This data is useful for research in space physics, magnetospheric physics, and upper atmospheric dynamics. All potential users must first get verbal approval from Dr. J.D.



BENCHMARKS FORUM is intended to serve as a vehicle for answering questions that may be of general interest to the user community. If you have a question, please send electronic mail to the Benchmarks editor (BITNET: AS04@UNTVM1) or write it down and drop it by the Computing Center. We will try to answer it in the next issue.

Question: What is the difference between a virus, Trojan Horse and a Worm?

Answer: A virus spreads by inserting itself into programs, causing them to insert it into even more programs. A trojan house, like the name implies, secretly does its dirty work while appearing to do something else. A worm propagates itself over networks, consuming network and connected computer system resources. Many articles in this issue of Benchmarks discuss these topics.§

Benchmarks Reader/User feedback is encouraged. Send all letters, suggestions, etc to (AS04@UNTVM1), FAX 817-585-4060 or to the Benchmarks Editor at:
Academic Computing Services
University of North Texas
Computing Center
NT Station,
Box 13495
Denton, Texas 76203



Winningham (512-522-3075). After receiving verbal approval, SDDAS is accessed by TELNET ESPSUN.SPACE.SWRI.EDU 540.

- SIMBAD - SIMBAD (Set of Identifications, Measurements, and

UUCP and UNT

At NT, the most popular way to be a part of these Usenet news groups is with the ANU program on the VAX Cluster. Through ANU, anyone with a VAX Cluster userid can take part in up to 366 different newsgroups. Messages from all over the world can be read from the user's terminal.

Usually this system works flawlessly, but a few weeks ago something happened. A computer and UUCP network node partially operated by AT&T called ATTCTC was seized by the US Secret Service as evidence in an ongoing nation-wide investigation of data piracy, credit card and long distance dialing abuse, and computer security violation called *Operation Sun Devil*. When that happened, the umbilical cord between NT and UUCP was severed.

An understanding of why this impacted NT requires an understanding of how UUCP works. The great strength and weakness of many wide area networks is their reliance on "store and forward" technology. Wide area networks which use store and forward schemes typically communicate only with computers, or nodes, that are geographically close to them. If a node on one side of the world has some e-mail, news or a file to send to a node on the other end of the world, it simply passes the data to a computer close to it along with instructions about the eventual destination. That computer, in turn, passes the data on to a computer close to it until, many nodes later, the e-mail, news or files reach their intended destination.

The great strength of this scheme lies in its economy. Any particular site need only pay for connections to a nearby neighbor to access the rest of the world. This way, a large number

of sites can affordably interconnect in a global wide area network.

The frailty of this technology is its weakness. On a network where the cost is so low to connect, many sites don't arrange redundant routing in case a critical node goes down. NT was such a site. When ATTCTC was seized, all the nodes "downstream" from it, including NT, lost their UUCP access. All these sites had to scramble to contact other geographically close UUCP nodes that were "upstream" of ATTCTC to arrange for new UUCP access. Three days later, thanks to the Computer Science department at the University of Texas at Austin, NT was back online to UUCP, but for some other sites on the UUCP network, the story was just beginning.

This account is based largely on the grand jury indictments against alleged Legion of Doom members and accounts by actual Legion of Doom members who posted to the Usenet group comp.dcom.telcom

The rest of the story¹

Sometime in December of 1988, Robert Riggs, a 20 year-old student of DeVry Technical School, hacked his way into a computer at Bell South

¹The story related in this section is based on the various sources cited at the end of this article. As this issue goes to press, the story is continuing to happen. The account of the events related here, although confirmed with two or three sources, is based on second-hand accounts and hearsay. Most of it is probably true. Some of it may not be. The best way to know for sure is to read the continuing first-hand accounts in Usenet newsgroups like `comp.dcom.telcom` (Telcom digest) in ANU on the VAXcluster.

telephone company headquarters in Atlanta. Bell South provides telephone service for Alabama, Mississippi, Georgia, Tennessee, Kentucky, Louisiana, North Carolina, South Carolina and Florida.

Riggs was a member of a group called the *Legion of Doom*. Members of this organization are hackers who illegally compromise the security of various computer and telecommunications installations on a regular basis in order to enhance their reputation within the computer underground.

Once he gained access to the Bell South computer, Riggs stole a document describing some of the workings of the emergency 911 service.² On 23 January, 1989 Riggs copied the file through the UUCP network

to Jolnet, a public access Unix system in Lockport, Illinois and made it available to Craig Neidorf, an editor of an underground on-line magazine for hackers and phreakers (hackers who specialize in compromising telecommunications security).

Phrack, the magazine edited by Neidorf, is published electronically through the UUCP and NSF-Internet networks and on numerous BBS's

across the country which specialize in disseminating information about hacking and phreaking. The magazine, a mainstream publication in the computer underground, is generally considered required reading for hackers and phreakers. The content of *Phrack* ranges from actual and fictional accounts of breaking into computer systems to technical details of computer security and tele-

²The Bell South name for the stolen computer text file is *Bell South Standard Practice (BSP) 660-225-104SV-Control Office Administration of Enhanced 911 Services for Special Services and Major Account Centers*.

In the years since 1985, when it began operation, Killer/ATTCTC became a critical node on the national UUCP backbone. Computers throughout the southwest, and people who used them, depended on ATTCTC for Usenet news, electronic mail and UUCP file transfer services.

communications systems. Sources close to the *Phrack* publishers assert that the magazine has always been careful to avoid publishing anything that was overtly illegal.

Neidorf, a 19 year old political science major at the University of Missouri, used his userid on a school unix system to retrieve the Bell South 911 file from Jolnet. Once he got the file, he edited it, as advised by Riggs, to conceal its source. Neidorf and Riggs intended to eventually write an article about the 911 system in *Phrack*.

The actual 911 file in question is a six page, 20 kilobyte document describing some technical and administrative details of the emergency 911 system that Bell South uses for its nine state service area.

Through the 911 system, Bell South customers can dial 911 and be instantly connected with a Public Safety Answering Point (PSAP). Computers called Electronic Switching Systems (ESS's) are critical to telephone routing. Once someone in the Bell South service area calls 911, an ESS ensures they are connected with an appropriate PSAP. The 911 system then allows an emergency operator to determine automatically what number and address the caller is calling from and alert the appropriate emergency service dispatchers.

Obviously, the details of security around such a system should be very closely guarded. The potential for loss of life and property if such a

system were maliciously compromised is enormous.

The Plot Thickens

Unknown to Riggs and Neidorf, Richard Andrews, the system administrator of Jolnet discovered the Bell South 911 file on his computer soon after it was transferred there. Andrews sent a copy of the file through the UUCP network to another computer system called "Killer" that was owned and operated by an AT&T employee, Charles Boykin. Andrews requested that Boykin forward the file to the appropriate authorities. Andrews

cooperating with the authorities ever since. It is largely through his cooperation that federal indictments have been returned against five alleged members of the Legion of Doom: Robert Riggs, Craig Neidorf, Adam Grant, Franklin Darden, Jr., and Leonard Rose.

On February 3rd, 1990, after receiving Andrews' cooperation for over a year, the Secret Service raided Jolnet and seized it as evidence.

Killer Falls

In 1989, the privately-owned UUCP node known as Killer, through which Richard Andrews alerted AT&T of the stolen 911 file, was moved to the Dallas Infomart. It was used by its owner, Charles Boykin, and AT&T as a public demonstration system. It was given a new name, *AT&T Customer Technology Center*, or ATTCTC. In the years since 1985, when it began operation, Killer/ATTCTC became a critical node on the national UUCP backbone. Computers throughout the southwest, and people who used them, depended on

AT&T claims that the closure was due to lack of funds, although the system was privately owned and operated by Charles Boykin. Sources close to the Texas Unix community assert that ATTCTC was shut down and seized by the US Secret Service . . .

didn't prevent further access to the file, delete it or frustrate the efforts of Riggs and Neidorf. He also kept a copy of the file for himself.

Several months later, Andrews received a call from someone at AT&T who asked for another copy of the file. Not soon after that, the United States Secret Service came paid him a visit. Andrews has been

ATTCTC for Usenet news, electronic mail and UUCP file transfer services. On the 20th of February, 1990, without any advance notice, ATTCTC was permanently shut down, leaving NT with no UUCP access.

AT&T claims that the closure was due to lack of funds, although the system was privately owned and

When all was said and done that day, the Secret Service had taken the Illuminati computer, all staff personal computers and printers, modems, software, spare hardware, all material related to GURPS Cyberpunk, a laser printer, a bag of nuts and bolts and some candy off the desk of Creede Lambard, who ran the Illuminati BBS.

operated by Charles Boykin. Sources close to the Texas Unix community assert that ATTCTC was shut down and seized by the US Secret Service because two of its usersids belonged to suspected members of the Legion of Doom. Various credit card numbers and long distance dialing codes were allegedly found in files owned by these usersids.

The Next Dominoes to Fall

In Austin, there's a small company called Steve Jackson Games that makes role playing games (a kind of grown-up make believe). In their offices, SJG ran a computer called Illuminati. This system was used by staff and customers to develop new game ideas. SJG ran a BBS on Illuminati though which customers could provide feedback based on testing of potential new games. One of these games was called *GURPS Cyberpunk*, named after the Cyberpunk genre of science fiction in which the plot often involves extensive penetration of computer security.

The author of *GURPS Cyberpunk*, Loyd Blankenship, researched ways in which to lend a realistic "look and feel" to his game. In his research, he developed extensive contacts with the hacker and phreaker underground, and acquired a comprehensive library of *Phrack* magazines, which he stored on Illuminati.

On the morning of March 1st, 1990, the staff of Steve Jackson Games arrived at work to find that the Secret Service had forced their way into the building and were searching and seizing "computer hardware and software and records relating to computer hardware and software" for evidence in a "nationwide data piracy case" which Steve Jackson later learned was the Bell South 911 case.

When all was said and done that day, the Secret Service had taken the Illuminati computer, all staff personal computers and printers, modems,

group Comp.dcom.telcom saying, among other things, that:

Frank [Darden, Jr.], Rob [Riggs] and Adam [Grant] were all definately [sic] into very hairy systems. They had basically total control of a packet-switched network owned by Southern Bell (SBDN) ... through this network they had access to every computer Southern Bell owned [...]

On April 1st, in *New York Newsday*, a story appeared saying:

A government affidavit alleged that in June hackers believed to be Legion of Doom members planted software "time bombs" in AT&T's 5 ESS switching computers in Denver, Atlanta and New Jersey. These programs ... were defused by AT&T security personnel before they could disrupt phone service.

So far, during the course of their investigation, the US Secret Service and the FBI have raided 27 computer sites across the US and have seized the equivalent of 23,000 computer disks from suspects accused of contributing to over \$50 million in system thefts and damages.

software, spare hardware, all material related to *GURPS Cyberpunk*, a laser printer, a bag of nuts and bolts and some candy off the desk of Creede Lambard, who ran the Illuminati BBS.

On the 20th of February, a member of the Legion of Doom who identified himself as "Erik Bloodaxe" posted an anonymous electronic mail message to the Usenet news

Elsewhere, Leonard Rose, sysop of a computer system called Netsys, was out driving his car one day when federal authorities pulled him over and arrested him. On the 15th of May, he was indicted with five felony counts and charged with various violations of interstate transportation laws and the federal Computer Fraud and Abuse act. Federal prosecutors allege that Rose hacked his way into an AT&T computer and

The Austin-based company Steve Jackson Games has been devastated by this affair. In the days since the Secret Service seizure, SJG has suffered a monetary loss of \$100,000, had to lay off 8 of their 17 staffers, and cancel sixty percent of their 1990 product releases.

stole some of the source code for version 3.2 of the Unix operating system. He is also charged with distributing two "trojan horse" programs that would infiltrate a Unix computer and replace the legitimate login program. Once in place, the trojan horses acquired a valid userid and password each time a new person logged into the system. Rose, it is alleged, would later retrieve the list of stolen userids and passwords and gain any degree of access to a system that he wanted.

So far, during the course of their investigation, the US Secret Service and the FBI have raided 27 computer sites across the US and have seized the equivalent of 23,000 computer disks from suspects accused of contributing to over \$50 million in system thefts and damages. The investigation continues into people who have violated the security of federal research centers, schools and private businesses, and extends far beyond the theft of a single six page text file from Bell South headquarters.

Craig Neidorf, the 19 year old University of Missouri student who allegedly received the 911 file from Robert Riggs, has pleaded not guilty to charges of violating the federal Computer Fraud and Abuse Act of 1986.

Charlie Boykin, the AT&T employee who ran Killer/ATTCTC and was initially alerted by Richard Andrews about the 911 file theft was previously an active member of the Texas Unix community. He hasn't been seen at any Unix function since the closure of ATTCTC.

According to the Associated Press, U.S. Attorney William Cook was granted a motion to prevent the 911 text file from becoming part of the public record during the trial. The trial of Riggs and Neidorf began on April 16, 1990.

The Austin-based company Steve Jackson Games has been devastated by this affair. In the days since the Secret Service seizure, SJG has suffered a monetary loss of \$100,000, had to lay off 8 of their 17 staffers,

tice system evaluates all property crime in monetary terms: if it doesn't cost a lot of money, then there's not a big crime involved.

The Chicago indictment against Riggs and Neidorf charges them with the theft and interstate transport of something valued over \$5,000, namely the 911 file.³ In other words, the crime lies in stealing something worth a lot of money, not potentially endangering the safety of people in nine states. Typically, computer crime is only investigated if a large monetary loss can be proven.

Some users and system operators of networked large multi-user systems would probably tell you that the big deal is that such computer systems aren't traditionally covered by common carrier statutes. Common Carrier laws are the laws that say if someone plots a crime over the telephone or through the US mail, the

Federal authorities are placing a burden of responsibility on owners and operators of such computers to know the legality of everything stored on their computer system. On a system such as the NT VAX Cluster, that means knowing completely what's on 4.3 gigabytes of disk storage, and reading over 100 megabytes of wide area network traffic each week.

and cancel sixty percent of their 1990 product releases. Jackson has approached the American Civil Liberties Union for assistance.

The Real Issues: What's the big deal?

That depends on who you ask.

The Secret Service would probably tell you that any violation of computer security is a serious affair. Unfortunately, the current criminal jus-

telephone company and the US Postal System cannot be held accountable for what was plotted over

³ Bell South values the six page 911 text file at \$79,499.00.

⁴Read Clifford Stoll's *The Cuckoo's Egg* [see page 7 for a review] for an excellent account of how federal authorities resisted involvement in violation of national defense computer security by a German hacker employed by the USSR because less than a million dollars in monetary loss was involved.

Someone would have to read up to sixty four thousand pages of text each week in order to be completely appraised just on new information that is either stored on the VAX cluster or passes through it on their way to another computer each week.

their common carrier. This is not the case with computer bulletin boards and network nodes, however. Federal authorities are placing a burden of responsibility on owners and operators of such computers to know the legality of everything stored on their computer system. On a system such as the NT VAX Cluster, that means knowing completely what's on 4.3 gigabytes of disk storage, and reading over 100 megabytes of wide area network traffic each week. In other words, someone would have to read up to sixty four thousand pages of text each week in order to be completely appraised just on new information that is either stored on the VAX cluster or passes through it on their way to another computer each week. If the NT Computing Center employed five people who could read 100 words a second to do this, and they worked twenty four hours a day without stopping, it would still take them twenty three days to read a week's worth of wide-area network traffic.

And to make matters worse, NT is, for all practical purposes, an end node on the wide area network circuit. Most traffic that passes through here is eventually bound for someone at NT. For most wide area network nodes, this is not the case. A site like UT at Austin, or Rice University has traffic passing through it, briefly being stored before being forwarded, for many national as well as international sites. For those sites, not only would they need to hire many more people, but

they would need to be foreign language interpreters as well.

Imagine a company that owns a telecommunications satellite being held responsible for all the conversations in all the languages that are going through it at all times. It's a ridiculous thought and no legal authority would expect that of RCA or NASA. However, the equivalent is expected of every BBS in the country and every wide area network node at this moment.

Unless lawmakers grant the same legal protection to computer bulletin boards and network nodes as the US Mail and telephone carriers,

There is a fine line between making a computer secure enough to avoid compromise by a hacker, and accessible enough not to discourage legitimate use.

computer users in the not-to-distant future will only be able to look back at the age of electronic mail and Usenet news.

People like the Legion of Doom have forced federal authorities apply existing laws to computers before they have sufficient technical preparation to do so. Unfortunately, it looks like the only solution to inappropriate seizures of computers by the Secret Service and FBI is the education that lawmakers and law enforcers will receive through the courts. Once more phreakers and hackers are ar-

rested and tried will it become apparent that seizing the computers they use as conduits makes as much practical sense as seizing the laser printer at Steve Jackson Games, not to mention the candy on Creede Lambard's desk.

In the case of computer security, the best and only effective offense is a good defense. No computer system is impregnable, but there is a point at which every hacker will decide that penetrating a system is more trouble than it's worth. It is especially important that all managers and system administrators of computer BBS's and network nodes be mindful of this.

Just as barbed wire spawned a burgeoning wire cutter market, the popularity and usefulness of computer-based communication will ensure that there are always going to be hackers and phreakers. There is a fine line between making a computer secure enough to avoid compromise by a hacker, and accessible enough not to discourage legitimate use.

The best managers of computer systems will continue to walk that line without disturbing the network of trust that makes such systems the powerful tools they are. §

Kevin Mullet is a data communication analyst in the NT Computing Center. He may be reached by electronic mail at KEV@VAXAACS.UNT.EDU. This article may be retrieved as a WP51 document by anonymous FTP or from the Novell network server, NTVAXB as a postscript source in file Doom150.ps

More Internet Databases

By Billy Barron, VAX System Manager
(BITNET: BILLY@UNTVAX)

This article is a continuation of the article that appeared in the April/May 1990 issue of *Benchmarks*. In the first article it was stated that the Internet is a collection of interconnected networks that span the world. It can be accessed through the VAXcluster or sometimes, through CMS Mail. Many databases containing information on a wide variety of topics are available to Internet users. Following are descriptions of some of these databases not covered in the previous article.

- **NETLIB** - Netlib is a library of public domain mathematical software. The software includes routines for linear algebra, benchmarking, curve fitting, FFTs, linear programming, differential equations solvers, non-linear optimization, and matrices. For more information, send a one line mail message to NETLIB@RESEARCH.ATT.COM. The line should contain SEND INDEX. NETLIB questions should be directed to Jack Dongarra (DONGARRAH@CS.UTK.EDU) at Oak Ridge National Laboratory and Eric Grosse (EHG@RESEARCH.ATT.COM) at AT&T Bell Labs.
- **OCEANIC** - The Ocean Network Information Center (OCEANIC) has a database of oceanographic information. This information is primarily used to support the World Ocean Circulation Experiment (WOCE), but is available to Internet users also. OCEANIC

Continued on page 18

THE BITNET CONNECTION

By Dr. Philip Baczewski, BITNET INFOREP (BITNET: AC12@UNTVM1)

This Column is a continuing feature of Benchmarks intended to present news and information on various aspects of the BITNET wide area network.

Sending Mail Over BITNET

Electronic mail is possibly the most frequently used BITNET service. Users of all three UNT mainframe systems (CMS, MUSIC, and VAX/VMS) are able to send mail over BITNET, using the mail facilities that are available on those systems. If you are not familiar with the mail facility on the mainframe system you are using, consult the help information available for that particular mail program. The following discussion centers on sending BITNET mail when using those facilities.

Sending and Receiving BITNET Mail on MUSIC

The MUSIC/SP MAIL facility can provide easy communication with other users of MUSIC, or with users of systems other than MUSIC (remote systems). These remote systems include CMS and the Vax Cluster, but also include any other BITNET nodes.

To use the MAIL facility, type MAIL SEND from MUSIC *GO mode. When you are prompted to enter the ID code for the receiver of the message, you must enter the receiver's BITNET address in the following format: `userid@node`, where `userid` is your correspondent's ID code and `node` is the remote system's BITNET node name. You can also specify a file name where a copy of your outgoing message is logged, whether or not you wish the message to be acknowledged, and if you wish the message text to be read from a file. Typing MAIL alone will cause the MAIL program to check your mailbox for messages and display any you have received.

The MUSIC MAIL facility also includes a program which allows you to specify nicknames for the BITNET addresses you use frequently. To create or modify a "names" file containing your list of nicknames, type NAMES from *GO mode. (For help within the NAMES program, use the PF1 function by pressing <ESC><1>). If, for example, you frequently send mail to LARRYW at NUS-DISCS, you could define the nickname LARRY to represent that address. To send mail to that address, you would only need to type LARRY in the To: field.

Because MUSIC limits the user-ID and node fields to the eight-character length imposed by RSCS, BITNET mail from MUSIC cannot usually be sent through gateways. Mail sent through gateways often has an address in which the user-ID and/or the node portion is longer than eight characters. There are techniques for specifying these addresses on both CMS and the VAX, however no provision for gateways is available on MUSIC.

It is especially important that if you frequently receive mail through BITNET, that you read, log (if desired), and purge mail DAILY. Failure to read and purge your BITNET mail on a regular basis can cause your mailbox to become full, cause messages to be "backed up" waiting to get into your mailbox, and possibly

GENERAL INFORMATION

Bibliography for Astronomical Data) is a database on astronomical objects. SIMBAD is accessible over the Internet, but requires an account to be set up. For more information about gaining access to SIMBAD, send E-mail to simbad@cfa.harvard.edu or call (617) 495-7301. §

Seminars Offered to Faculty, Staff

By Claudia Lynch, *Benchmarks* Editor
(BITNET: AS04@UNTVM1)

Each semester, classes are offered by Academic Computing Services' Microcomputer Support staff for the University Personnel Office's Training and Development Program "Hands-On Computer Seminars." These seminars are available to all faculty and staff members. According to information provided by the Personnel Office: "Your participation in Personnel-sponsored programs is considered a part of your working hours, and your supervisor's approval is required for you to register for training if you are a staff member. A record of the programs you attend is a part of your permanent personnel file."

Contact the Personnel office for more information and to register for the following classes that are being offered this summer:

- Introduction to Microcomputers and DOS.
- Introduction to WordPerfect.
- WordPerfect 5.1 Conversion.
- Introduction to PlanPerfect. §

1990 Summer Short Courses

Academic Computing Services
University of North Texas
Computing Center

The Computing Center is offering the following short courses for the 1990 summer semesters. Please pre-register to attend (a registration form can be found at the end of this issue). A maximum of 10 people will be admitted to each of the courses held in ISB 110. A maximum of 7 people will be admitted to each of the courses held in the Graphics Lab. A maximum of 8 people will be admitted to each of the courses held in ISB 123.

PLEASE NOTE: Faculty and students have first priority to register for these classes. staff members ** MUST ** register through the personnel office.

MAINFRAME COURSES

1. **Introduction to MUSIC/SP** - MUSIC/SP is an interactive operating system employed by academic users to access the Academic HDS/8083 IBM-compatible mainframe computer at UNT. MUSIC is primarily used to submit batch jobs to the MVS operating system, providing access to a variety of programming languages and several statistical analysis packages. Topics covered include gaining access over the Local Area Network, logging on and off, changing your password, and creating, editing, and storing files using the full-screen editor. Additional topics that may be covered, depending on available time, are: accessing on-line help facilities, using electronic mail, routing output to high-speed printers, and writing files to secondary storage such as disk and tape.

Introductory sessions to MUSIC/SP will be held in Room 110 of the Science Library (ISB) on a bi-weekly basis. **NO PRE-REGISTRATION IS REQUIRED FOR THESE COURSES.** Consult the **HELP DESK** (565-4050) for a schedule of classes and/or to request a class on a specific day. All courses will be taught by Help Desk staff.
2. **Introduction to IBM Job Control Language (JCL)** - This course provides an overview of IBM JCL for users who wish to further their knowledge in

GENERAL INFORMATION

this area. It is useful to individuals who plan to run batch jobs (e.g. SAS, SPSS-X) on the IBM-compatible mainframe computer.

A two-hour session to be held in the Academic Computing Conference Room (ISB 123):

- Monday, June 11: 3-5 p.m.
Instructor: George Morrow

3. **Introduction to SAS** - SAS is one of the most widely implemented data analysis systems within business and education. SAS is particularly well suited for dataset manipulation and includes an extensive procedure library providing a wide range of analytical tools. This course is recommended for individuals who plan to incorporate statistical analyses into their research. Topics covered include the reading of data into SAS, simple data transformations recoding variables, labeling output, and performing simple univariate and bivariate analyses.

A two-hour session to be held in the Academic Computing Conference Room (ISB 123):

- Friday, June 8:
10:30 a.m.-12:30 p.m.

Instructor: Panu Sittiwong

4. **Introduction to SPSS-X** - SPSS-X is the latest version of this popular data analysis system originally developed for social scientific research. While SAS is slightly more powerful for the analysis of complex datasets, many users find SPSS-X to be easier to learn. SPSS-X also includes more flexible facilities for collapsing and labeling variables. This course is recommended for individuals who plan to incorporate statistical analyses into their research. Topics covered include the reading of data into SPSS-X, simple data transformations, recoding

variables, labeling output, and performing simple univariate and bivariate analyses.

A two-hour session to be held in the Academic Computing Conference Room (ISB 123):

- Friday, June 15:
8:30-10:30 a.m.

Instructor: Phanit Laosiriratt

5. **Introduction to CMS** - CMS is an interactive operating system employed by academic users to access the Academic HDS/8083 IBM-compatible mainframe computer at UNT. CMS users have access to a variety of programming languages, a sophisticated text processing system, and several statistical analysis packages. Topics covered include gaining access over the Local Area Network, logging on and off, changing your password, and creating, editing, and storing files using the full-screen editor. Additional topics that may be covered, depending on available time, are: accessing on-line help facilities, using electronic mail, and routing output to high-speed printers.

A two-hour session to be held in the Academic Computing Conference Room (ISB 123):

- Friday, June 8:
8:30-10:30 a.m.

Instructor: Phillip Baczewski

6. **Introduction to VAX/VMS** - VMS is the interactive operating system used on the Digital Equipment Corporation (DEC) VAXcluster. The VAXcluster supports a variety of applications. The topics covered in this course include gaining access to the VAXcluster through the Local Area Network, logging in and out, changing your password, creating files and

directories, creating login command files, using the EDT editor, defining logicals and symbols, and electronic mail.

A two-hour session to be held in the Science Library (ISB 110):

- Friday, June 8:
8:30-10:30 a.m.

Instructor: Mark Thacker

7. **Introduction to BITNET** - BITNET is a network linking more than 600 computers at over 300 institutions and research centers. This course covers the basic concepts of BITNET, file transfers across BITNET sites, and other services that are available on this computer network. Faculty and graduate students needing to exchange information with other universities and research institutions in the U.S., Canada, Europe, or Japan will benefit greatly from attending this course. Prior knowledge of at least one of the following interactive operating systems is required: CMS, MUSIC, VAX/VMS.

A two-hour session to be held in the Academic Computing Conference Room (ISB 123):

- Friday, June 15:
10:30 a.m.-12:30 p.m.

Instructor: Phillip Baczewski

7. **Introduction to the Internet and THENET** - The Internet is a collection of realted computer networks that link thousands of computers throughout the world. THENET is a network that connects universities, research institutions, and state agencies in the state of Texas. This course covers basic concepts, file transfer, remote login, and other services available on the networks. Faculty and students needing to exchange information with other universities, government agen-

GENERAL INFORMATION

cies, companies and research institutions or between the various machines on the University of North Texas campus would benefit from this course. Prior knowledge of at least one of the following interactive operating systems is required: VAX/VMS, Unix, MS-DOS, MAC.

A two-hour session to be held in the Academic Computing Conference Room (ISB 123):

- Friday, June 22:
10:00 a.m.-Noon
Instructor: Billy Barron

MICROCOMPUTER COURSES

1. Introduction to Microcomputer Labs: ISB 110, Willis Library, Graphics Lab - Special emphasis is placed on the unique features of networked microcomputers in these labs. Topics such as accessing file servers and printing to remote printers available to UNT students will be covered.

Two separate one-hour sessions to be held in the Science Library (ISB 110):

- Monday, June 11:
3:30-5:30 p.m.
Instructor: Staff
- Wednesday, July 11:
3:30-5:30 p.m.
Instructor: Staff

2. Introduction to Microsoft Word - Basic word processing in a Macintosh environment using Microsoft Word.

A two 1/2 hour session to be held in the Graphics Lab (ISB 6):

- Friday, June 22:
10 a.m.-12:30 p.m.
Instructor: Pro Systems Staff



Remember ...

Faculty members can request "customized" short courses for their classes. Call 565-2324 for more information. §

3. Introduction to WordPerfect, Version 5.1 - An Introduction to the major features of WordPerfect 5.1 including cursor movement, deleting and inserting, changing margins and spacing, using current system date, blocking and moving, speller, thesaurus and printing documents. Prior knowledge of basic DOS commands required. Bring one 5 1/4" low density formatted diskette. There is no difference between WP 5.1 and 5.0 at the Introductory level. If you are comfortable with 5.0 do not take this class.

A three-hour session to be held in the Science Library (ISB 110):

- Friday, June 29:
9 a.m.-Noon
Instructor: Sandy Franklin

4. Introduction to Procomm Plus - An overview of the Procomm communications package for Personal Computers or compatibles is presented. Procomm provides several different terminal emulation modes, and supports several file transfer protocols including KERMIT and XMODEM. Topics covered include setting communications and file transfer parameters, setting up and using Procomm's dialing directory, and connecting to UNT host computers through the local area network.

A one-hour session to be held in the Academic Computing Conference Room (ISB 123):

- Friday, June 22: 9-10 a.m.
Instructor: Anto Prijosoesllo

5. Introduction to SAS PC - This course covers the basics of using SAS PC, Version 6.03, for IBM and compatible PCs. Topics covered include using the SAS Display Manager, loading files, selecting variables and running statistical analyses. Emphasis will be placed on running SAS in interactive mode. Prior knowledge of the SAS command language or attendance in the Intro to SAS course is required.

A three-hour session to be held in the Science Library (ISB 110):

- Friday, June 8:
10:30 a.m.-12:30 p.m.
Instructor: Phanit Laosirirat

6. Introduction to SPSS PC+ - This course covers the basics of using SPSS PC+, Version 3.1, for IBM and compatible PCs. Topics covered include using the menu and help interfaces in REVIEW, loading files, selecting variables and running statistical analyses. Emphasis will be placed on building files for execution interactively. Prior knowledge of the SPSS-X command language or attendance in the Intro to SPSS-X course is required.

A three-hour session to be held in the Science Library (ISB 110):

- Friday, June 15:
10:00 a.m.-Noon
Instructor: Panu Sittiwong §

Maczilla -vs- the Slime Monsters

or

Computer Virus Prevention on the Macintosh

By Chad Irby, Microcomputer Support Consultant (BITNET: ACH@UNTVAX)

Macintosh computers are well-known for being easy to use. They are also well-known for being the first computers to suffer under the virus plague of the 1980s. There are several different strains of Macintosh viruses, but so far, none of them have done the severe damage found in the MS-DOS world.

The public access microcomputer labs at the University of North Texas have been host to almost all of the various Macintosh viruses, and we assume that we will see more as time goes by. In the last six months, we have seen these strains:

- INIT 29
- nVIR
- ANTI
- Scores
- WDEF A & B

Most of the Mac viruses are designed to be harmless, but due to poor design by the virus programmers (frequently known as scum), they often cause odd system problems.

Typical behavior of an infected Macintosh

- Problems with printing — locks up or can't open printer.
(Often caused by INIT 29 infections)
- Unexplained beeps on startup.
(nVIR does this at random times)
- Disk drive problems (Scores virus creates extra invisible files and fills drive)
(INIT 29 causes *This disk needs minor repairs* message when the disk is OK)
- Macintosh Portable or IICI crash on insertion of floppy disk.
(WDEF virus can cause this sometimes)
- Mouse pointer moves erratically across screen.
(ZUC virus — not seen in this area yet, see article in adjacent column).
- Unexplained system crashes.
(Most viruses can cause this — INIT 29 does this a lot)

How to deal with the problem

There are several products which can help you deal with Macintosh computer

Continued on page 23.

Macintosh ZUC Virus

By Mike McCann, Clemson University
(MMCCANN@HUBCAP.CLEMSON.EDU)

This article is excerpted from the DICT Update (Vol. 13, #5, May 1990), the newsletter of the Clemson University Division of Computing and Information Technology. Another Mac menace, a trojan, is described on page 28. — ed.

The latest virus to infect the Macintosh community is the ZUC virus (named after its discoverer, Don Zucchini). This virus was discovered in Italy in March 1990 and infects applications only (applications do not have to be run to become infected). Once an infected application is run, the cursor bounces around the screen uncontrollably when the mouse button is depressed.

Some of the following problems have been reported:

- Desktop patterns may change.
- Slower launching of applications with increased disk activity.
- The virus spreads between file servers and Macintoshes.

There are two ShareWare programs which are commonly used to get rid of the ZUC virus, *Disinfectant 1.8* and *GateKeeper*.

- *Disinfectant 1.8* is used to disinfect Macintosh diskettes and hard drives from all current Macintosh viruses including ZUC. *Disinfectant 1.8* must be run before it can work since it is an application not an INIT or CDEV.
- *GateKeeper* is an INIT which is placed in the System Folder and used to detect and prevent infection from the ZUC virus. §

Maczilla continued from page 22

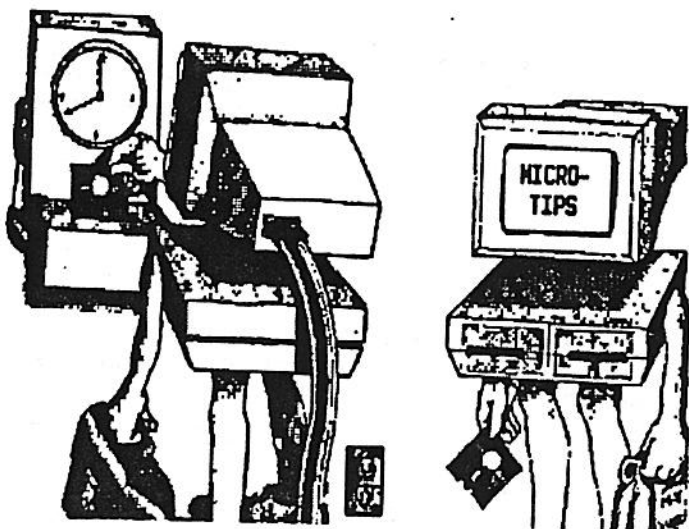
viruses. The most popular one is *Disinfectant*, a program by John Norstad of Northwestern University. *Disinfectant* is a free program which scans entire volumes for viral activity, then eliminates any infections it finds. Typical time for inspection of a hard drive is about a minute. It is a very useful tool to own, and is updated every time a new strain is found. The current version (1.8) is available through the Macintosh labs here at the University. Another free program, *Vaccine*, will help prevent infections from happening, but won't catch the newest bugs.

GateKeeper is free, and can prevent most infections, but takes more time to set up. It has the advantage of locking out any unfamiliar system activity, so it has caught several new viruses (the recent MDEF strain, for example) before anyone knew they existed. It is not a product for beginners, since the user has to configure it for the programs most commonly used on that machine.

The most common commercial program for virus prevention is SAM, or *Symantec Antivirus for the Macintosh*. SAM scans the hard drive on startup, and automatically inspects each floppy when you insert it into the drive. SAM is relatively easy to set up, and can be trained to check for new strains as they come along. SAM is available at most Macintosh software outlets at various prices. §

WordPerfect Users Group Meetings

The UNT WordPerfect Users Group will continue to meet every third Friday from 12 to 1 p.m. in Marquis Hall, Room 105. All WordPerfect users are invited to attend. §



This column is intended to serve as a forum for sharing useful tips on making more productive use of microcomputers. If you have a tip that you feel may be of use to campus users, submit it to the Benchmarks editor for possible inclusion in a future issue.

Establishing Meaningful Relationships

By Kyle Capps, Manager of Microcomputer Support

Dbase III Plus and Dbase IV are relational database management systems, but many people do not understand the significance of the word "relational" and even fewer people have actually used this very powerful feature of Dbase. The April/May 1990 *Benchmarks* Micro-Tip involved the creation of a relational database to store invoicing information. This month's Micro-Tip "brings it all together" into a program that will print invoices from the invoice master database.

Bringing It All Together

We will assume that some invoice information has been entered into the databases INVMASER and INVITEM to illustrate how the relations work at the printing of the invoice. The short program that is provided below assumes that you are somewhat familiar with the Dbase programming language and the program is compatible with both Dbase III-Plus, Dbase IV, and the Clipper compiler.

Program Analysis

A complete invoice printing program would be much more complex than the program listed on the following pages, but the program does provide the examples needed to understand relational database designs. In the program provided, we have established several relations between databases as outlined on page 27.

Invoice Program Listing

```

*
* PROGRAM NAME : INVPRINT.PRG
* SYSTEM      : INVOICE.PRG
* AUTHOR      : KYLE F. CAPPS
* DATE WRITTEN : 04/12/90
* VERSION     : 1.0
* COMMENTS    : THIS PROGRAM IS USED TO PRINT INVOICES FROM THE INVOICE MASTER DATABASE.
*               THE PROGRAM WILL UTILIZE THE DATABASES INVMASTER,INVITEM,CUSTOMER,COMPANY,
*               SHIPPER, AND PRODUCT TO PRINT THE INVOICES.
*
*

```

```

*
* OPEN ALL DATABASES (ASSUMES THAT ALL INDEXES WERE PREVIOUSLY CREATED)
*

```

```

select 1
open invmaster.dbf index invmaster.ndx alias invmaster
select 2
open invitem.dbf index invitem.ndx alias invitem
select 3
open customer.dbf index customer.ndx alias customer
select 4
open company.dbf index company.ndx alias company
select 5
open shipper.dbf index shipper.ndx alias shipper
select 6
open product.dbf index product.ndx alias product

```

```

*
* ESTABLISH RELATIONS BETWEEN DATABASES
*

```

```

select invitem
set relation to invoice_no into invmaster, item_code into product
select invmaster
set relation to cust_code into customer, ship_code into shipper, comp_code into company

```

```

*
* CREATE LOOP TO PROCESS RECORDS IN INVITEM.DBF
*

```

```

select invitem
goto top
rowpos = 60
page_no = 1
sub_total = 0
weight_total = 0
ship_chg = 0
tax = 0
total = 0
curr_invoice_no = invitem-invoice_no
do while .not. eof()
  select invmaster
  if invmaster-print_sw = "Y"

```

```

&& Row number variable
&& Page number counter
&& Subtotal variable
&& Shipping weight total
&& shipping charges
&& Tax rate for customer
&& Grand total variable
&& Store invoice no to memory variable

```

```

&& Check if invoice has been printed

```

```

*
* SKIP TO NEXT RECORD
*

```

MICROCOMPUTERS

```

else
    select invitem
    skip +1

*
* PRINT THE INVOICE
*
select invitem
set device to print                && Direct output to printer
if rowpos 55 .or. curr_invoice_no invitem-invoice_no  && Check if new page
*
* CHECK FOR NEW INVOICE NUMBER
*
if curr_invoice_no invitem-invoice_no  && New invoice number
    @ rowpos + 1, 50 say "_____ "
    @ rowpos + 2, 40 say "Subtotal: "
    @ rowpos + 2, 50 say sub_total picture "$99999999.99"
    @ rowpos + 3, 40 say "Shipping: "
    @ rowpos + 3, 50 say weight_total * ship_chg
    @ rowpos + 4, 40 say "Tax Total: "
    @ rowpos + 4, 50 say sub_total * tax
    @ rowpos + 5, 50 say "_____ "
    @ rowpos + 6, 40 say "Total : "
    total=subtotal+(weight * ship_chg)+(sub_total * tax)
    @ rowpos + 6, 50 say total picture "$99999999.99"
    curr_invoice_no = invitem-invoice_no
else
    page_no = page_no + 1
endif
*
* PRINT NEW PAGE HEADING AND TOP PART OF INVOICE
*
rowpos = 1                        && Reset row counter
eject                            && Execute form feed
do PRINT_TOP
rowpos = 24                      && Reset row counter
sub_total = 0                   && Reset subtotal
total = 0                      && Reset grand total
ship_chg = shipper-weight_chg   && Get new shipping charges
tax = customer-tax_rate         && Get new tax rate
endif
@ rowpos + 1, 3 say invitem-qty
@ rowpos + 1, 9 say product-item_code
@ rowpos + 1, 22 say product-item_desc
@ rowpos + 1, 38 say product-unit_price
@ rowpos + 1, 50 say product-unit_price * invitem-qty
sub_total = sub_total + (product-unit_price * invitem-qty)
skip +1
rowpos = rowpos + 1

endif
enddo (while .not. eof())
*
* PROCEDURE TO PRINT THE TOP PART OF THE INVOICE
*
PROCEDURE print_top
    @ rowpos,(80 - len(trim(company-comp_name)))/2 say trim(company-comp_name)
    @ rowpos + 1,(80 - len(trim(company-comp_addr1)))/2 say trim(company-comp_addr1)

```


MICROCOMPUTERS

```

if trim(company-comp_addr2) = ""                                && No second address
    addr_line = trim(company-comp_city)+", "+company-comp_state+" "+trim(company-comp_zip)
    @ rowpos + 2,(80-len(addr_line))/2 say addr_line
    @ rowpos + 3,(80-len(trim(company-comp_phone))/2 say trim(company-comp_phone)

else
    @ rowpos + 2,(80-len(company-comp_addr2))/2 say trim(company-comp_addr2)
    addr_line = trim(company-comp_city)+", "+company-comp_state+" "+trim(company-comp_zip)
    @ rowpos + 3,(80-len(addr_line))/2 say addr_line
    @ rowpos + 4,(80-len(trim(company-comp_phone))/2 say trim(company-comp_phone)

endif
@ rowpos + 6, 55 say "Invoice Number : "
@ rowpos + 6, 71 say invmaster-invoice_no picture "@B"
@ rowpos + 8, 55 say "Invoice Date : "
@ rowpos + 8, 71 say invmaster-inv_date
@ rowpos + 10, 55 say "Page Number : "
@ rowpos + 10, 71 say page_no picture "@B"
@ rowpos + 12, 10 say customer-bill_name
@ rowpos + 12, 45 say customer-ship_name
@ rowpos + 13, 10 say customer-bill_addr1
@ rowpos + 13, 45 say customer-ship_addr1
if trim(customer-bill_addr2) = ""                                && No second address
    addr_line = trim(customer-bill_city)+", "+customer-bill_state+" "+trim(customer-bill_zip)
    @ rowpos + 14 ,(80-len(addr_line))/2 say addr_line
    @ rowpos + 15,(80-len(trim(customer-bill_phone))/2 say trim(customer-bill_phone)

else
    @ rowpos + 14,(80-len(customer-bill_addr2))/2 say trim(customer-bill_addr2)
    addr_line = trim(customer-bill_city)+", "+customer-bill_state+" "+trim(customer-bill_zip)
    @ rowpos + 15,(80-len(addr_line))/2 say addr_line
    @ rowpos + 16,(80-len(trim(customer-bill_phone))/2 say trim(customer-bill_phone)
endif
if trim(customer-cust_addr2) = ""                                && No second address
    addr_line = trim(customer-ship_city)+", "+customer-ship_state+" "+trim(customer-ship_zip)
    @ rowpos + 14 ,(80-len(addr_line))/2 say addr_line
    @ rowpos + 15,(80-len(trim(customer-ship_phone))/2 say trim(customer-ship_phone)

else
    @ rowpos + 14,(80-len(customer-ship_addr2))/2 say trim(customer-ship_addr2)
    addr_line = trim(customer-ship_city)+", "+customer-ship_state+" "+trim(customer-ship_zip)
    @ rowpos + 15,(80-len(addr_line))/2 say addr_line
    @ rowpos + 16,(80-len(trim(customer-ship_phone))/2 say trim(customer-ship_phone)

endif
@ rowpos + 18, 0 say "P.O. Number   Terms       Sales Person       "
@ rowpos + 19, 2 say invmaster-cust_po_no
@ rowpos + 19,20 say customer-terms
@ rowpos + 19,38 say invmaster-salesman
@ rowpos + 20, 0 say "_____ "
@ rowpos + 21, 0 say "Ship Date   Shipper"
@ rowpos + 22, 2 say invmaster-ship_date
@ rowpos + 22,14 say shipper-ship_name
@ rowpos + 23, 0 say "_____ "
@ rowpos + 24, 0 say " Qty  Item Number  Description                Unit Price  Ext. Price"

return

```

Program Analysis continued from page 23

Database Relations

Parent	Child	Link
INVITEM	INVMASER PRODUCT	INVOICE NO ITEM_CODE
INVMASER	CUSTOMER SHIPPER COMPANY	CUST_CODE SHIP_CODE COMP_CODE

As you can see from the above listing, a database can serve as both a "parent" and a "child" depending on the active database at the time. The significance of establishing relations is that all of the record pointers in the child databases move to the desired record depending on the link established between the parent database. This eliminates the use of multiple SEEK statements and simplifies program design.

Conclusion

Database relations represent an extremely powerful tool to the database developer and when utilized with a good initial database design, they become indispensable as an efficient means to manipulate multiple databases. §

Safe Computing Thwarts Viruses

By Susan Hay, Brown University.

This article originally appeared in The OPEN WINDOW (vol 2 no 6, May 1989—Brown University, Editor: Kirsten Robinson, KIRSTEN@BROWNVM.BROWN.EDU). It was received from the Articles database of CCNEWS, the Electronic Forum for Campus Computing Newsletter Editors, a BITNET-based service of EDUCOM. The article was altered to reflect local procedures at UNT.

Many campuses have had problems recently with hostile programs spreading throughout the computing community. These programs invade a computer system and can destroy data, applications, and even hardware. Due to the steady growth of personal computer use, hostile programs have become a concern for all of us. Fortunately, there are a number of things you can do to help prevent damage to your system.

What hostile programs do

There are three major types of hostile programs currently in circulation: viruses, trojan horses, and worms. A virus inserts itself into other programs and, when executed, inserts itself into even more programs. In this way it spreads from disk to disk, computer to computer. It may also erase files, crash systems, or display harassing messages. Viruses often stay dormant for a period of time

before doing their dirty work to ensure their spread to other systems before being detected. A trojan horse, like its namesake, secretly executes one function while appearing to accomplish some other task or pretending to be some other program. For example, DANCERS.BAS shows animated dancers in color on your IBM PC screen and secretly wipes out your hard disk's file allocation table (FAT) at the same time. (DOS needs the FAT to access files.) Finally, a worm replicates itself over a network, consuming network and large-system resources. The internet worm which was in the news this past fall spread through a network to defense, commercial and educational computers across the country, bringing down whole systems in its wake.

Different hostile programs are bigger threats on different machines. In the DOS world, trojan horses are by far the most prevalent. The Macintosh, however, has been suffering lately from a host of highly contagious virus infections. Worms have been restricted to larger systems so far and usually don't affect the average microcomputer user.

Common sense tips

There are several things that microcomputer users can do to protect their systems from harm.

- First, never use original, or master, diskettes; use backup copies. When you first unpack the disks, write-protect them. Then make backups and put the originals in a safe place. If there is ever any question about the integrity of your applications, they can be compared to the masters and reinstalled if necessary.
- Make backups on a regular basis. Two or three times a week is not too often. In addition, keep two versions of your backups: a recent copy and one a month old. That

way if your most recent backup is compromised, you have an older version from which you can restore your data.

- When using a shared machine, first turn the machine off, wait a second, and then turn it back on. This is called a cold boot (in a warm boot, the machine is restarted but the power is not turned off). Virus code can "live" in the computer's memory and transfer itself to the next disk that is inserted. Only by turning the machine off can you guarantee that nothing is lurking in memory.
- Make sure you know where your software comes from. Do not use public domain software without ensuring that it is clean. Download software only from reputable bulletin boards that check all software before uploading it. A warning—viruses have made their way into commercial software. Do not assume that because the program was shrink-wrapped that it is virus-free. Unfortunately, there is no such thing as a tamper-resistant seal for software!
- Write-protect all system and application diskettes before inserting them. This will prevent viruses and trojan horses from writing to these disks. Be careful; a hostile program can check to see if a disk is locked and then print a message saying "this disk needs to be repaired—please unlock it." If you get a message like this, don't unlock the diskette; try a different one. If you get the same message, suspect an infection. Some software must be on an unlocked disk to run and cannot be protected this way. Instead, lock individual files using the Lock option in the Get Info window on the Mac, or the ATTRIB.COM program on DOS systems. These software locks are less dependable, however, as it is possible for a virus to bypass them.
- Watch for unusual changes in icons, file sizes or date stamps, especially in the System files on the Mac and the COMMAND.COM, IBMDOS.COM, and IBMBIO.COM files on the PC. Some viruses can be detected this way.

Prevention, detection and eradication

As fast as viruses are being discovered, programs called vaccines are being written to detect and protect against them. These vaccines try to anticipate various ways that a virus can infect your system, but none can guarantee to prevent infection. Even worse, virus authors can examine vaccine programs and write viruses to circumvent them. Because of this competition between viruses and vaccines, be sure to periodically update any vaccine for the most effective virus protection. Virus protection and eradication software for both Macintoshes and IBMs is available from the Help Desk or the Graphics Lab.

If you think your diskette is infected or damaged, you can bring it to the Computing Center and a microcomputer consultant will help you. If your hard disk is affected, make an appointment with a microcomputer consultant (565-2316) to bring your machine in to be checked. We will do our best to help you recover your files and/or eradicate infection.

Be careful out there!

Hostile programs have become a serious concern for microcomputer users, but there is no need to panic. With a little care and caution, it is possible to greatly reduce the risk of damage by viruses or trojan horses. §

Nasty Mac Trojan

Discovered in Canada

Taken from an article in Turn-Around-Times (Vol. 19, #3, Spring 1990), the newsletter of the Computing Center at the University of California at Davis.

A deadly Macintosh trojan has been going around that destroys everything on your hard disk, renames the hard disk "Gotchal," and then destroys any unlocked floppies in your disk drives. Currently, the best way to protect yourself is to immediately make backups of your hard disks and floppy disks. There is no telling when and where this virus might hit, but if or when it does, it will be more than just annoying.

The trojan was detected most recently in Canada at the University of Alberta. Two different strains have been identified. Both are dangerous.

The first strain is embedded in a program called "Mosaic" (Type=Appl and Creator=???). When launched, it immediately destroys the directories of all available physically unlocked hard and floppy disks, including the one it resides on. The trojan also mounts and destroys any unmounted but available SCSI hard disks. All disks are renamed "Gotchal!"

The second strain has been detected in a public domain program called "FontFinder" (Type=APPL and Creator=BNBW). It has a trigger date of February 10, 1990. On or after the trigger date, the trojan is invoked and disks are attacked in the same manner as the first strain.

After an attack by either version, you usually can recover files off hard disks with one of the available commercial file utility programs, but often the data file names are lost.

If you have a copy of SAM Anti-Virus Utilities, use it. If not, get one. §

Protecting Your Computer Hardware & Peripherals From Theft

Much of the information in this article was taken from an article by the same name written by Ivars Balkits (BITNET: ISBALKITS@UCDAVIS), Computing Services, University of California, Davis. The text of Mr. Balkits article was received from the Articles database of CCNEWS, the Electronic Forum for Campus Computing Newsletter Editors, a BITNET-based service of EDUCOM.— ed.

Microcomputers are a popular theft item. Just this past semester, the College of Music was hard hit by the theft of their \$6,500 Macintosh II computer. In November of 1989, thieves hit both the Music Annex and the Marketing Department. They stole an IBM PC from the Music Department and a Macintosh SE from the Marketing Department. Off-campus, it is not uncommon to read about microcomputer thefts in the "Police Blotter" section of various newspapers, including the *Denton Record Chronicle*. This article attempts to incite interest in more effective means of securing campus computers against loss through theft. It provides basic tips and tricks for managing computer security, describes those lockdown devices, and lists resources of information on theft protection and specifics on recommended anti-theft devices.

Managing Computer Security

A first step to managing computer security on campus is an awareness of people who belong in your work area and those who do not. Challenge any strangers. People posing as repairpersons often walk off with computers. Demand identification and proper documents prior to allowing the removal of any hardware from your office or lab. Report any suspicious people to Campus Police at 565-3000.

Deterrents to computer theft both on and off campus include: key control, lockdown devices, regular security checks, alarm systems, and proper insurance coverage (to ameliorate loss when thefts do occur).

- **Key control** — Locking the door to your office or an unattended lab when you leave is an important beginning to effective theft prevention. Dead bolt locks are highly recommended. Key control also means not distributing too many copies of a key, as well as accurately documenting that distribution.
- **Lock-down devices** — A lockdown device should have no exposed cables. If the cable can be clipped with pliers or wire cutters or loppers and the computer can thus be removed, the device is not secure. Any locking device with exposed aluminum bolts is also unsecure.
Lockdown devices for computer equipment comprise four types:
 - 1) steel wrap-around units that enclose the computer and are secured by locks, bolts, and/or adhesive pads or plates.
 - 2) one or more steel plates glued or bolted directly to the computer and a support such as a desk.
 - 3) glue-on patches secured by cable and padlock.
 - 4) various screw-on or glue-on extras (swivels, shelves, tilt adapters, cooling fans, etc.).
- **ID markings** — Engraving the words "Property of" your name and your social security number is highly recommended. Most police departments

have electric engraving devices that you can borrow.

- **Alarm systems** — Though costly, an alarm system connected to a police station can be an effective theft-deterrent. It can lead to the capture of the perpetrator, as well as recovery of the stolen equipment.
- **Vendors** — Some vendors of anti-theft devices are Versa Lock, Inc., Business Machine Security (BMS), and Anchor Pad International. FMJ Inc. and T-Track Systems also distribute anti-theft devices. Prices of the devices range from around \$37 to over \$250. Less expensive cable systems are also available.

Check with your local computer store for more detailed information about anti-theft devices. If you are concerned about your equipment on campus, contact Microcomputer Support in the Computing Center (565-2316) or Micro Maintenance (565-2387). The personnel in those departments will be able to advise you about specific steps to take to secure your equipment.

NOTE that many lockdown devices are used not only on computers, but microwaves, calculators, centrifuges, scales, and other lab equipment.

References

- "College seeks stolen computer." *The North Texas Daily*, Vol. 73, No. 104, April 18, 1990.
- "Computer Theft." *ucla Microcomputing* (UCLA), Vol. 4, No. 6, November-December 1988. p. 12.
- "Is Your Computer Secure?" *Systems* (UC Riverside), Vol. 8, No. 1, October 1988. p. 1.
- "Physical Security of Microcomputers." *UofSER News* (University of Saskatchewan) Vol. 18, No. 9, September 1987. p. 27.8

VAX Upgrades

By Billy Barron, VAX System Manager (BITNET: BILLY@UNTVAX)

The VAX operations staff, as is their custom, installed many software upgrades including a few with new and exciting features. They are as follows.

- **WIN/TCP** — WIN/TCP version 5.1 was installed. This new version includes many new features.

First FTP is 20% faster. Now if you anonymous FTP into VAXB.ACS.UNT.EDU, you will notice that it supports CD and there are more files available. These files include many megabytes of public domain and shareware microcomputer programs.

The Unix TALK utility is now available on VMS. TALK is similar to VMS PHONE, the major difference being that PHONE supports DECnet networks and TALK supports TCP/IP networks such as the Internet. To use TALK, just type TALK userid@nodename from the \$ prompt. For example, use the command TALK JESUS@EMX.UTEXAS.EDU to talk to Jesus at the node EMX.UTEXAS.EDU. For more information on TALK, type HELP TALK from the \$ prompt.

Version 5.1 has a menu driven interface to the TCP software and an Online Tutorial. Both can be accessed by typing RUN TWG\$TCP:[NETDIST:TUTORIAL]WINMENU from the \$ prompt.

Finally, this version supports several new system management functions and remote printing over TCP/IP. Though we currently don't use this printing func-

tion, we will use it in the future to share printers between VMS and Unix systems.

- **VAX Pascal** — VAX Pascal 4.0 is a major upgrade of VAX Pascal. Version 4.0 incorporates many of the features of the new extended Pascal standard, which is currently in draft form, including:

- **Schema Types** — The schema data type is a fairly new development in the Pascal language. The major advantage is being able to generate array lengths at run-time instead of compile time. For example,

```
TYPE
  Unit_numbers(Len : INTEGER) =
    ARRAY [1..Len] OF INTEGER;
```

```
VAR
  Machines : Unit_numbers(10);
  Devices : Unit_numbers(A);
```

The above line that defines the variable "Machines" is equivalent to the following old VAR statement:

```
VAR
  Machines : ARRAY[1..10] OF
    INTEGER;
```

The line that defines the variable "Devices" was impossible to duplicate under the old version of VAX Pascal. "Devices" will be an array of integers with A elements in the array. The key though is that A is a variable which allows the program to decide how big the array should be at run-time.

String schemas are also available. VAX Pascal now has a predefined schema known as STRING, which behaves like the type

VARYING OF CHAR. For example,

```
VAR S : STRING(A);
```

will create a VARYING OF CHAR variable with length A. The above examples only cover the simplest uses of the Schema data type.

- **Short Circuit Logic** — For a long time, the biggest criticism of VAX Pascal has been that it doesn't support short circuit logic correctly. Due to a bug and backwards compatibility reasons, VAX Pascal previously did not support short circuit logic. VAX Pascal 4.0 introduces two new operators called AND THEN and OR ELSE that guarantee left-to-right evaluation with short circuit logic. In most cases, it is advisable to use AND THEN instead of AND and OR ELSE instead of OR.

- **Initial State Specifiers** — Initial state specifiers allow a variable or data type to have an initial value. The initial value must be a constant though. For example:

```
TYPE
  Initially_Zero = INTEGER
  VALUE 0;
```

```
VAR
  I : Initially_Zero;
  Valid : BOOLEAN VALUE
  FALSE;
  Pi : REAL VALUE 3.14;
```

In these examples, "I" has an initial value of 0, valid is initially false, and Pi is initially 3.14.

- **Enhanced Constructors** — A constructor is a list of values used to assign values to structured objects, such as arrays, records, and sets. Constructors existed in previous ver-

sions of VAX Pascal, but with version 4.0 their functionality has greatly increased.

First of all, constructors now allow indices and fields to be explicitly specified. For example:

```
TYPE
  A = ARRAY [1..10] OF
    INTEGER;
  R = RECORD
    F1: INTEGER;
    F2: REAL;
  END;
CONST
  CA = A[1..5: 42; 6..10: 84];
  CB = R[F1: 42; F2: 3.14];
```

In this example, elements 1 through 5 of CA have the value of 42. Elements 6 through 10 have the value of 84. Field F1 of record R has the value 42 and field F2 has the value of 3.14.

```
CONST
  CC = A[1,3,5,7,9: 42;
    OTHERWISE 0];
```

Elements 1, 3, 5, 7, and 9 have the value of 42. The other elements of CC (2,4,6,8,10) have the value of 0.

Also, constructors can be used in assignment statements. For example:

```
VAR
  VA: A;
FUNCTION Random: INTEGER;
EXTERNAL;
VAR EXTERNAL VAR:
  [EXTERNAL] Integer;
BEGIN
  VA := A[1,3,5,7,9: Random;
    OTHERWISE External_var];
END
```

In this example, the odd elements get the value of function Random. The even element get assigned the value of the variable External_var.

- **UPPER and LOWER Functions** — The LOWER and UPPER functions have been extended to handle the upper and lower bounds of ordinal types, set base types, and array index types. For multidimensional arrays, a second parameter can be specified to indicate the dimension. For example:

```
TYPE
  AT = ARRAY [1..10] OF
    INTEGER;
BEGIN
  WRITELN(LOWER(AT),
    UPPER(AT));
END
```

would print 1 and 10 to the screen.

- **FOR IN Statement** — The FOR IN statement allow the selection of each item from a set expression. For example,

```
FOR I IN [1,3,5,6] DO
  Writeln(I);
```

would print the numbers 1, 3, 5, and 6 on the screen.

- **Non-decimal Integer Constants** — A new notation is now included to specify integer constants in any base from 2 to 36. The syntax is:

base#extended-number

Some examples:

```
2#1001001
8#3777
16#FEED
```

- **Array-Indexing and Field Selecting FUNCTION results** — Functions returning structured types, such as arrays or records, can now be indexed or selected directly instead of requiring the use of a temporary variable. For example:

```
TYPE
  Array_Type = ARRAY [1..5] OF
    INTEGER;
  Record_Type = RECORD F1:
    REAL END;
FUNCTION Array_Fn: Array_Type;
EXTERNAL;
FUNCTION Record_Fn:
  Record_Type; EXTERNAL;
BEGIN
  WRITELN(Array_Fn[3],
    Record_Fn.F1);
END
```

In the past, you would have had the following code segment to achieve the same results:

```
VAR
  A: Array_Type;
  R: Record_Type;
BEGIN
  A := Array_Fn;
  R := Record_Fn;
  WRITELN(A[3],R.F1);
END
```

Many other new VAX Pascal features exist. For a full description of the new features, see the file SYSSHELP:PASCAL040.RELEASE_NOTES on the VAX.

- **Netware VMS** — Netware VMS has been upgraded to version 2.1 from 2.0A. This will lend to greatly increased connectivity with the rest of the Novell Internet on the UNT campus. The SHELL.CFG files that were needed for compatibility with the old version of Netware VMS are no longer needed.

One side effect of the Netware upgrade is that the VAX and Netware VMS passwords will be independent from now on (i.e. if you change your VAX/VMS password, your Netware VMS password does not change). Unfortunately, the Netware upgrade procedure did not carry forward existing passwords to the new version of Netware. Therefore, all Netware VMS passwords have been reset to the original password of the account (i.e. the

password on the slip of paper you got when your account was assigned). If you don't what that password is and need it, come by the Computing Center and have it looked up or changed.

Version 2.1 supports CAPTURE. Hopefully in the future, CAPTURE will allow some printer sharing between PCs and the VAX. In addition, the new version supports all the features of Netware 2.13.

- **Other upgrades** — The other upgrades recently installed are Ada 2.1, BASIC 3.4, VAX C 3.1, COBOL 4.3, FORTRAN 5.4, Lisp 5.1, Minitab 7.2, and VMS 5.3-1. These upgrades mostly consisted of bug fixes instead of new features. §

BEST OF THE BBS

Edited by Mark Thacker,
VAXProgrammer/
Operator (BITNET:
MARK@UNTVAX)



Welcome to the Best of the BBS column. This column highlights some of the more interesting and useful discussions on the UNT BBS. For those of you not familiar with the BBS, here is how to log into the UNT BBS.

- Sign-on by typing CALL DEC at the LAN prompt and then entering BBS as your Username at the VAX prompt.
- If you are already logged-on to the VAXcluster, type BBS at the \$ prompt.

VAXCLUSTER USAGE STATISTICS

April Top Ten Programs: CPU Time Used

Program	Description	CPU Time	Percent of Total
1. User programs	Compiled Programs	41 23:33:26.58	83.9
2. NEWS	ANU News Utility	1 10:37:37.92	2.9
3. LISP	Lisp Interpreter	1 01:12:31.73	2.1
4. EDT	Editor	0 14:10:56.81	1.2
5. PASCAL	Pascal Compiler	0 10:57:39.55	0.9
6. BACKUP	Disk Backups	0 10:47:48.79	0.9
7. NNTP_TCPWIN	News Transfer Utility	0 08:35:05.27	0.7
8. MAIL	VMS Mail	0 07:02:58.75	0.6
9. LOGINOUT	User login	0 06:42:17.96	0.6
10. BBS	Bulletin Board	0 06:27:07.98	0.5
Total		50 01:17:24.49	

April Top Ten Programs: Frequency of Runs

Program	Description	Number of Runs	Percent of Total
1. LOGINOUT	User login	68440	17.1
2. SET	VMS Utility	55232	13.8
3. User programs	Compiled Programs	31640	7.9
4. DIRECTORY	VMS Utility	30099	7.5
5. DELETE	VMS Utility	29991	7.5
6. EDT	Editor	22336	5.6
7. SYSLOGIN	User Login	15778	3.9
8. SEND	Bitnet Message Utility	14170	3.5
9. TYPE	VMS Utility	13492	3.4
10. PASCAL	Pascal Compiler	11968	3.0
Total		401001	

The opinions expressed in this column do not necessarily reflect the views of Academic Computing Services or the Computing Center. Also, information in Best of the BBS has not been checked for accuracy.

PC Pursuit Access in Denton

#40417 5-APR-1990 12:13:30.09

Subject : PC Pursuit

Is there a way to connect to PC Pursuits dial ups from Denton? Without it being long distance? If so, does anyone have the number?

#40425 Reply to #40417 5-APR-1990 15:39:28.12

Subject : RE: PC Pursuit

Hi. Good question. No, there is not. There is another service however, which has the no charge local number, and which serves the same function as PCP. It's called Starlink. Talk to Chuck Reed on Visitor's; there is information there about it.

Two Line Headers in WordPerfect 5.0

#40459 6-APR-1990 11:26:28.04

Subject : HEEEEEEELP!

VAX COMPUTER CLUSTER

I have Wordperfect 5.0. I am writing a paper and my prof INSISTS that we have not only page numbers in the right top corner, but ALSO a short title on the line below the number! I can get WP 5.0 to give me either one, or both on the SAME line, but not as:

1
SHT TITLE
as I need it. Anybody have any ideas?
.....

#40461 Reply to #40459 6-APR-1990 11:57:26.66

Subject : RE: HEEEEEEELP!

Assuming that you are familiar with the WP program itself:

Under the format menu (shift-f8), then Page menu, there is a header option. Defining a header will allow you to do what the professor is asking for.

Select header, define header a, then edit. Here's where it gets interesting. Put a ^B (that's control-b to you and me) wherever you want a page code, then add whatever text you want. This text does *not* have to be on the same line as the page number! 8) When finished editing, press F7 and the return to the document.§

COMPUTING TECHNICAL SERVICES

Isolation, Redundancy, Key to Mainframe Security

By Claudia Lynch, Benchmarks Editor (BITNET: AS04@UNTVMI)

The University of North Texas maintains two separate IBM-compatible HDS-8083 computers for administrative and academic mainframe computing. These machines are electronically distinct, allowing academicians access to a variety of national and international wide area networks, while ensuring the integrity of administrative programs and data.

These computers are housed in a physically secure location, accessible by a combination lock. The combination is changed at regular intervals, and there are operations personnel on duty twenty-four hours a day.

The area that houses the computers is equipped with a halon fire smothering system and all equipment is connected to an uninterup-

table power supply, housed elsewhere in the building.

Protection from unauthorized persons tampering with programs and data or gaining physical access to the computers are very real concerns. The ability to maintain operations during adverse conditions is also an important aspect of security planning. The Computing Center has a very detailed *Disaster Recovery Plan* that specifies exact procedures to be followed in the event of natural or man-made disasters. These procedures go into effect when something happens to affect computing to such a degree that operations would have to be discontinued for more than 21 days.

An important aspect of the Disaster Recovery Plan involves off-site storage of data. All academic and administrative disk volumes are

backed-up to tapes at regular intervals (see "Disk Backup Schedules" at the end of this issue for some examples). The backup tapes are cycled so that they are housed in a fire-resistant vault on campus, then to an off-site storage facility in the metroplex, then back to a fire-resistant vault on campus. Each cycle takes a week. At the end of the third week, the tapes are put back into the UNT tape library. Such a system provides redundancies in backups in case there is a disaster of such a magnitude that more than one set of backup tapes is needed to restore operating systems and data to the point closest to the way they were before the disaster occurred.

Obviously, a great deal of time, effort and expense has gone into ensuring that both the academic and administrative mainframes will remain operational, even under adverse circumstances. This may not seem that important, at first, but consider the alternatives. If there is a system failure, is it acceptable to have to wait days or weeks for your paycheck or your grades or the results of the data analysis for your dissertation? Probably not.§

COMPUTING TECHNICAL SERVICES

Mainframe Performance Statistics

Operating Systems Performance Statistics for April

CPU	SYSTEM	Planned Production Hours	Production Hours Achieved	System Uptime
ACAD	VM/SP5	720.00	705.40	98.0%
ACAD	MUSIC/SP	682.30	665.46	97.5%
ACAD	MVS/JES2	720.00	695.95	96.7%
ACAD	COMPLETA	707.67	682.80	96.5%
ADMN	MVS/JES2	719.65	717.70	99.7%
ADMN	COMPLETA	267.00	266.08	99.7%
ADMN	ADABASA	689.50	682.17	98.9%

- The ACAD CPU achieved 100% uptime in April.
- The HDS/7360 DASD achieved 100% uptime in April.
- The HDS/7380 DASD achieved 100% uptime in April.
- The ADMN CPU achieved 100% uptime in April.
- The HDS/7360 DASD achieved 100% uptime in April.
- The HDS/7380 DASD achieved 100% uptime in April.
- The EMC Solid State Disk achieved 100% uptime in April.

Key Causes Of Lost Productivity In April: ADMN CPU

Miscellaneous

1. DASD file maintenance on ADABAS.	2.06 HOURS
2. Operator mistakes in system restarts.	1.53
3. Keeping COMPLETA down to run FISCAL jobs.	0.92
4. Systems software development.	0.80
5. MPU clocks set to daylight saving time.	0.78
6. ADABASA system failure.	0.28
TOTAL	6.37 HOURS

Key Causes Of Lost Productivity In April: ACAD CPU

CPU, Tape, and Disk Subsystems (HDS)

1. Research and analysis of incompatibility problem with MVS/SP running under VM/SP5 in dual-processing mode on the 8083. 8.15 HOURS
 2. Research and analysis of abortive attempts to load an alternate VM/CMS nucleus for evaluating performance of the EMC SSD disk unit. 3.57
 3. Cable in the EMC SSD disk unit for evaluating performance of this device on the 8083. 3.25
- TOTAL 14.87 HOURS**

Miscellaneous

1. Abortive attempts to load an alternate VM/CMS nucleus for evaluating performance of the EMC SSD disk unit. 5.43 HOURS
 2. Systems software development. 5.07
 3. Step missed in MUSIC backup procedure. 1.18
- TOTAL 11.68 HOURS**

GRAND TOTAL 26.55 HOURS

COMPUTING TECHNICAL SERVICES

April Top Ten Programs : Frequency Of Runs

Program	Description	#of Runs	% of Total
1. PGM=*DD	Compiled Program	11368	15.5
2. IEWL	Linkage Editor	10615	14.5
3. IEBGENER	IBM Utility	8505	11.6
4. ADARUN	ADABAS Utility Module	6542	8.9
5. SASLPA	SAS	4900	6.7
6. IGYCRCTL	VS COBOL2 Compiler	4251	5.8
7. SPCHLCOB	COBOL2 Report Writer	3489	4.8
8. IKFCBL00	VS COBOL Compiler	3215	4.4
9. SPSSX	SPSS-X	3051	4.2
10. IEV90	Assembler H	2662	3.6

April Top Ten Programs: CPU Seconds Used

Program	Description	CPU Seconds	% of Total
1. COMPLET4	Academic COM-LETE	132631	35.3
2. SASLPA	SAS	59854	15.9
3. PGM=*DD	Compiled Program	55700	14.8
4. ADARUN	ADABAS Utility Module	36381	9.7
5. SPSSX	SPSS-X	19875	5.3
6. SPCHLCOB	COBOL2 Report Writer	18050	4.8
7. IGYCRCTL	VS COBOL2 Compiler	8513	2.3
8. IEWL	Linkage Editor	5763	1.5
9. SSS4001	Operations Automation	4749	1.3
10. IKFCBL00	VS COBOL Compiler	4115	1.1

The programs listed in this section were used the most frequently on the HDS ACADemic CPU during April, 1990. Please Note that ACAD is the official designation of the HDS/8083 CPU that is dedicated to faculty and student use. The HDS/8083 CPU reserved for University administrative purposes is termed ADMN.§

Just for Fun: Literary Criticism Meets COBOL

By Jonathan R. Partington (JRP1@phoenix.cambridge.ac.uk). Received from the rec.humor.funny Newsgroup

A team of American scholars have performed a detailed computer analysis and they confirm that the language COBOL was invented by William Shakespeare (and not by Bacon, Elizabeth I, Walter Raleigh, Marlowe, Ben Johnson, or Don Knuth.) Taking a large sample of known COBOL programs, and works by the above authors, they performed a detailed analysis and confirm that COBOL matched the Shakespearean style almost perfectly. It also enabled them to identify various other works as COBOL programs which were previously thought to be poetry. For example the following is now known to be a genuine COBOL program.

"Let us ADD our INCOME to our CAPITAL, as the squirrel adds to its autumn horde. Aye, there's the SUM that makes a TOTAL EEALTH. 3000 DUCATS? Is this an EXPENDITURE I see before me? WEALTH. 3000 DUCATS? Is this an EXPENDITURE I see before me? Marry 'tis best 'twere TAKEN AWAY, like as the magpie taketh away the jewel of great price. But hist! Here

cometh the INTEREST, and 'tis of no mean interest, i' faith! I had lief ADD a percentage of this, than clasp my fair Rosalind's spleen."

Scholars have occasionally suspected that COBOL programs are supposed to have a 'hidden agenda', rather than being straight works of art in themselves. One bizarre theory is that they may contain numerical calculations embedded in them — indeed some scholars claimed that a Baconian cipher was involved. This seems implausible however.

Analysis of FORTRAN programs is next on the list — can 'Into the Valley of Death GOTO 600' really be by Alfred Lord Tennyson, or is just a pastiche of his style? Nobody knows for sure.

On the other hand, scholars are fairly sure that the C language was devised by James Joyce — mainly because, like Joyce, most of it is totally unreadable. §

COMPUTING TECHNICAL SERVICES

Disk Backup Schedules

SYSTEM	BACKUP	DESCRIPTION
Administrative MVS/SP	Daily	Monday - Friday around 7 p.m. (after COM-LETE is shut down) & on Saturday & Sunday if COM-LETE has been up that day.
	Weekly	Full pack dumps taken each Sunday morning.
	Monthly	Full pack dumps taken on the first day of each month.
Academic MVS/SP	Daily	Monday - Sunday during the early hours of the morning.
	Weekly	Full pack dumps taken each Sunday.
	Monthly	Full volume dumps taken on the first day of each month.
MUSIC/SP	Daily	Wednesday - Monday starting at 4 a.m. and lasting about 30 minutes.
	Weekly	Tuesday mornings at 3 a.m., these last about 2 hours.
	Semester	Once a semester, a permanent backup is taken.
VM/SP	VM Weekly	Early every Wednesday morning.
	CMS mini-disks	Daily backup performed early every morning. Weekly backup every Wednesday starting at 3 a.m.
VAXcluster	Daily	Incremental backups are performed Monday - Thursday at 6 p.m.
	Weekly	Full backups are performed every Friday beginning at 8 a.m. and generally last all day.
	Monthly	A "stand alone" backup is performed monthly. Dates and times are given in the system log-on message.
	Semester	Once a semester, a permanent backup is taken.

A full description of the system backup procedures can be found by typing **HELP BACKUP** on MUSIC/SP or the VAXcluster.



**University
of North
Texas
Computing
Center**

Richard A. Harris, Associate Vice President for Computing
Steve Minnis, Director of Computing Technical Services
Dave Molta, Director of Academic Computing
Coy Hoggard, Director of Administrative Computing
Claudia Lynch, *Benchmarks* Editor
Philip Baczewski, *Benchmarks* Associate Editor

Computing Center Short Course Registration Form

Please complete this form and return it AS SOON AS POSSIBLE if you wish to attend any of the short courses listed below. You may also register over the phone by calling (817) 565-2324. **FACULTY AND STUDENTS HAVE FIRST PRIORITY TO REGISTER FOR THESE CLASSES. STAFF MEMBERS ** MUST ** REGISTER THROUGH THE PERSONNEL OFFICE.**

NAME: _____ FACULTY ___ STAFF ___ STUDENT ___

DEPT: _____ UNDERGRADUATE ___ GRADUATE ___

PHONE: _____ MAILING ADDRESS: _____

SUPERVISOR SIGNATURE _____

I wish to attend:

● Introduction to JCL (ISB 123):

___ Monday, June 11: 3-5 p.m.

● Introduction to SPSS-X (ISB 123):

___ Friday, June 15: 8:30-10:30 a.m.

● Introduction to VAX/VMS (ISB 110):

___ Friday, June 8: 8:30-10:30 a.m.

● Introduction to the Internet & THENET (ISB 123):

___ Friday, June 22: 10 a.m.-Noon

● Introduction to Microsoft Word (ISB 6):

___ Friday June 22: 10 a.m.-12:30 p.m.

● Introduction to Procomm Plus (ISB 123):

___ Friday, June 22: 9-10 a.m.

● Introduction to Microcomputer Labs (ISB 110):

___ Monday, June 11: 3:30-5:30 p.m.

___ Wednesday, July 11: 3:30-5:30 p.m.

● Introduction to SAS (ISB 123):

___ Friday, June 8: 10:30 a.m.- 12:30 p.m.

● Introduction to CMS (ISB 123):

___ Friday, June 8: 8:30-10:30 a.m.

● Introduction to BITNET (ISB 123):

___ Friday, June 15: 10:30 a.m.-12:30 p.m.

● Introduction to WP 5.1 (ISB 110):

___ Friday, June 29: 9 a.m.-Noon

● Introduction to SAS PC (ISB 110):

___ Friday, June 8: 10:30 a.m.-12:30 p.m.

● Introduction to SPSS PC+ (ISB 110):

___ Friday, June 15: 10 a.m.-Noon

I would like to see more classes offered: ___ on weekends; ___ at night.

The classes I am interested in are: _____



**Academic Computing Services
The Computing Center
NT Box 13495
University of North Texas
Denton, TX 76203
FAX 817-565-4060**

Get a Subscription to *Benchmarks*

Benchmarks is a vital link between the UNT Computing Center and the users of our facilities. It is important for all users of the computing facilities to maintain a file of these newsletters because they contain materials which will periodically update existing documents as well as information and suggestions on uses of OS/MVS, MUSIC/SP, the VAXcluster, Microcomputers, and other resources available to UNT students and faculty. To facilitate the dispersal of *Benchmarks*, *** FREE *** subscriptions are available. To receive yours, send the following information to us either by snail mail (the post office or campus mail), FAX (817) 565-4060, or through electronic mail, to the UserID AS04 on MUSIC, VMS, or CMS.

Name: _____

Mailing Address: _____

PLEASE GIVE A CAMPUS ADDRESS (NOT BOX) IF POSSIBLE! - It's Cheaper !!

☐ Renewal ☐ Change of Address ☐ Cancel Subscription



Academic Computing Services

The Computing Center

NT Box 13495

University of North Texas

Denton, TX 76203

FAX 817-565-4060
